Introduction to Cybersecurity

Cybersecurity Fundamentals

Learning Objectives

By the end of lessons you will be able to:

- Explain the fundamentals of cybersecurity
- Identify threat actors, attacks, and mitigation
- Describe security policies, procedures, standards, and baseline
- Elaborate the cybersecurity mitigation methods

Fundamentals of Cybersecurity

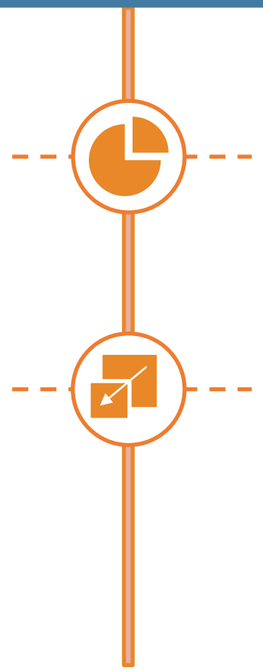
What Is Cybersecurity?

A set of technologies used for protecting systems, networks, and programs from digital attacks, damage, and unauthorized access.

Why Cybersecurity?

Information Security and Cybersecurity

Information Security	Cybersecurity
Refers to processes and tools designed to protect sensitive information	Is a set of techniques used to protect the integrity of networks, programs, and data
Encompasses paper documents and digital and intellectual property	Is a component of information security



Cyber Crime Statistics

25+ million records exposed everyday in 2018

Cyber Crime to cost $6 trillion in 2021

Healthcare: Ransomware attacks will quadruple

300 billion passwords exist worldwide in 2020

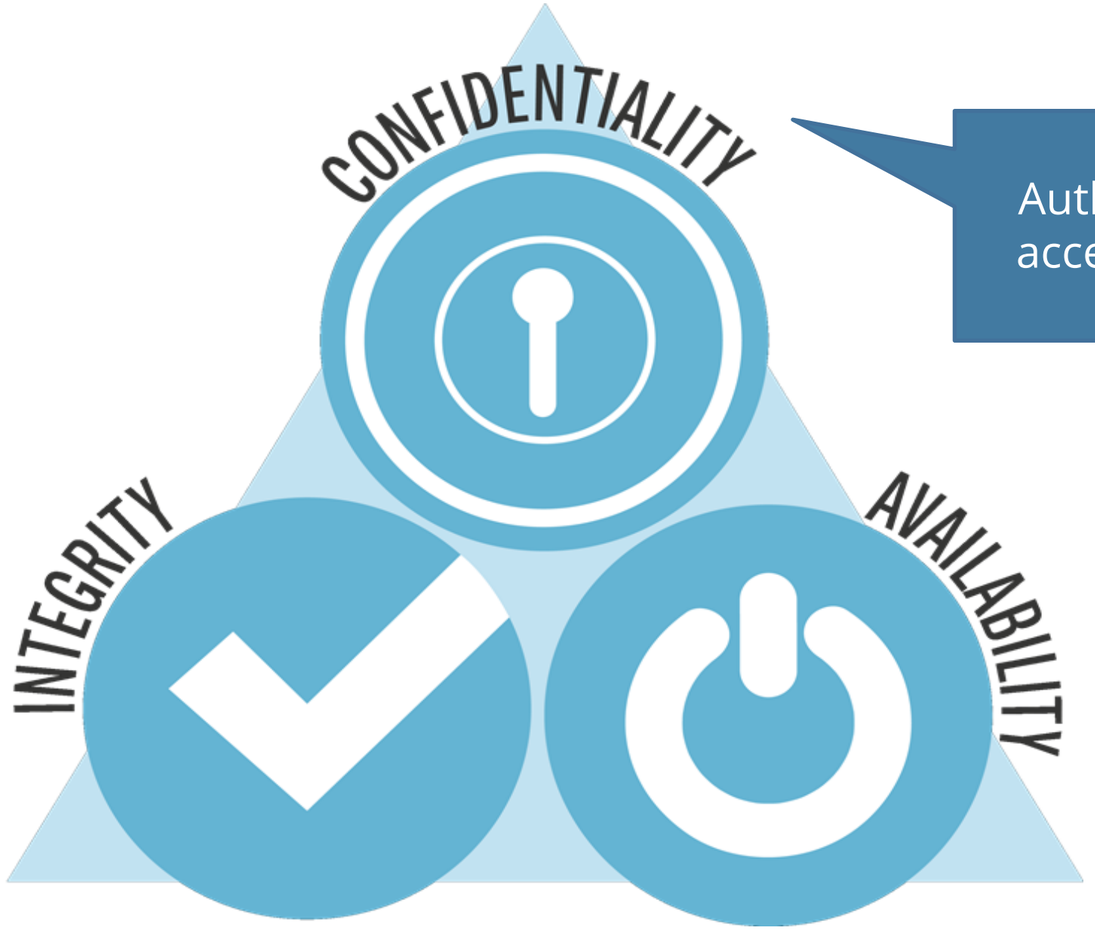
24,000 malicious mobile apps blocked daily

60% of fraud originates from mobile devices

Factors Affecting Cybersecurity

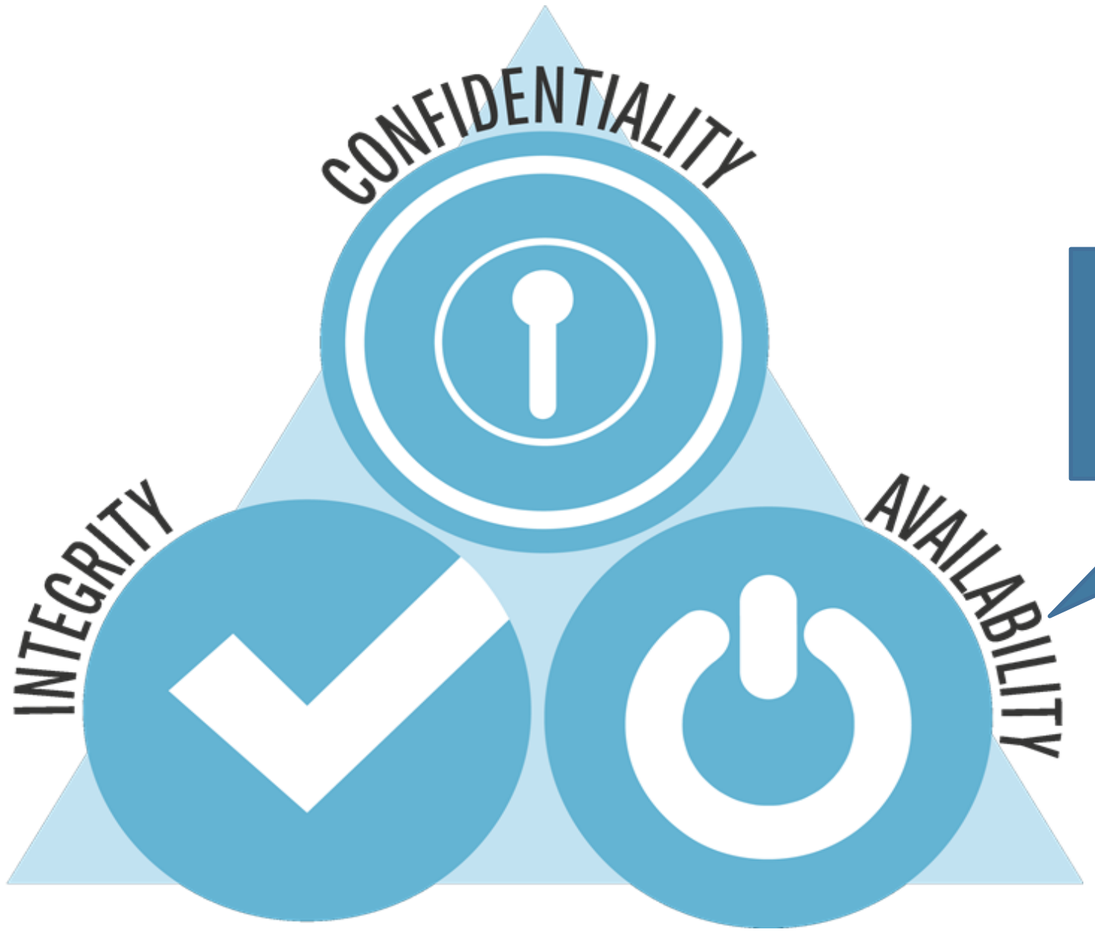
Technology		Business Plans
Platforms and tools	1	Nature of business
Network connectivity	2	Risk tolerance
Level of IT complexity	3	Industry trends
New or emerging security tools	4	Mergers and acquisitions and partnerships
Operational support for security	5	Outsourcing service providers

CIA Triad



Authorized parties can access the information

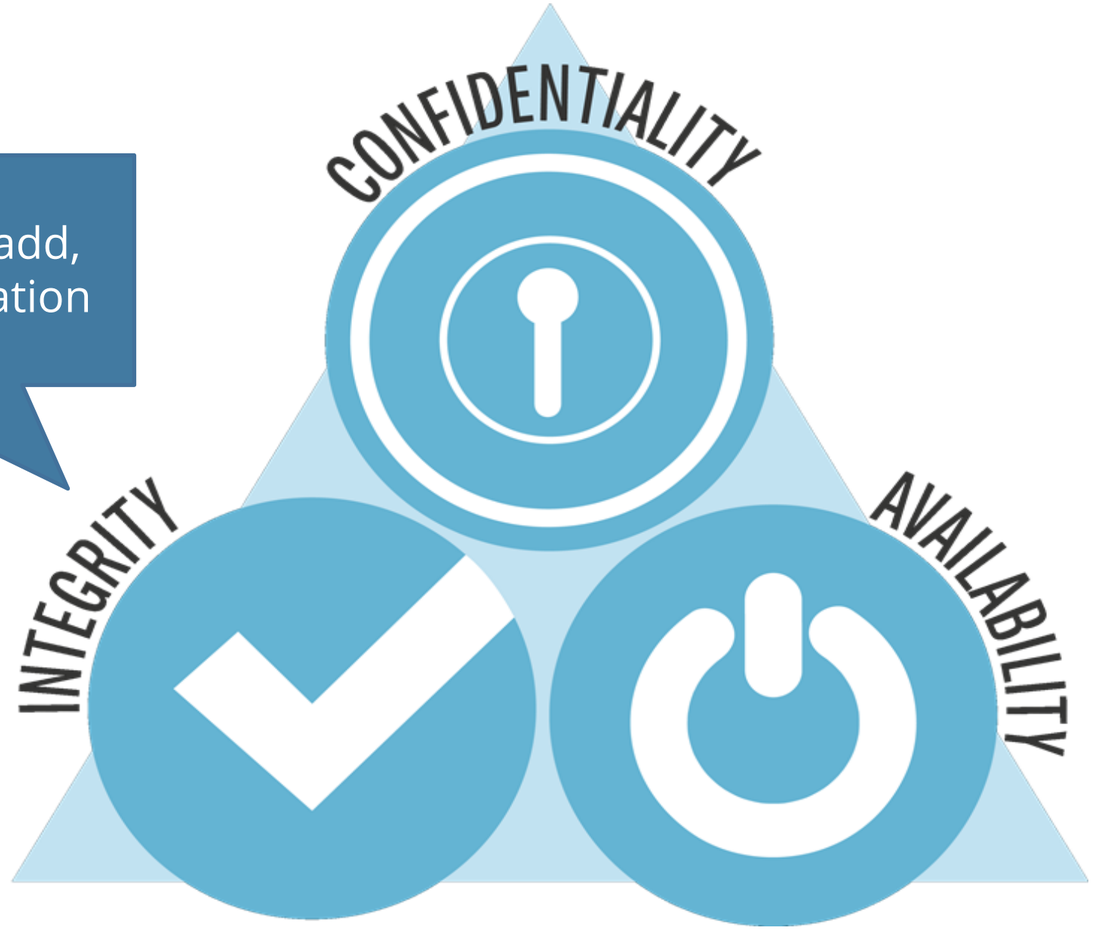
CIA Triad



Information must be available on demand

CIA Triad

Authorized people can add, remove, or alter information



Governance, Risk Management, and Compliance (GRC)

Scope of GRC

Governance, Risk Management, and Compliance of every organization is different and varies based on the type of organization.

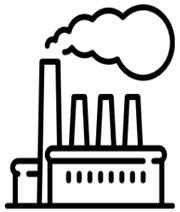
It depends on organization mission, size, industry, culture, and legal regulations.

Mission

Regulations

Size

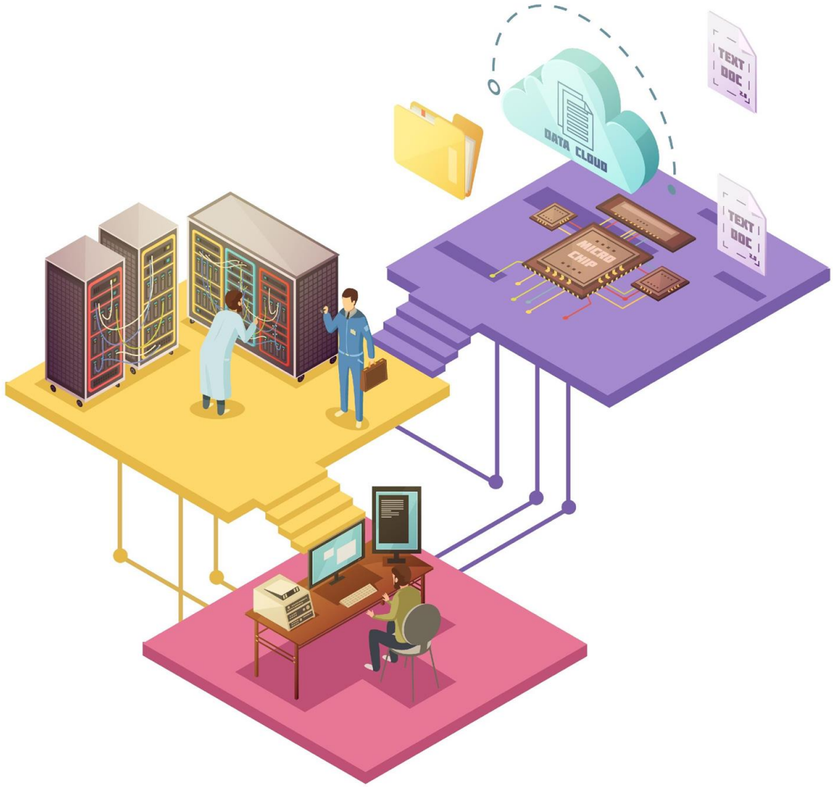
Culture



Industry

Responsibility of GRC

The ultimate responsibility of the GRC program is to protect their assets and operations IT, including their infrastructure and information.



GRC

Governance

Risk Management

Compliance

The board of directors and senior management of an organization are responsible for Governance.

- Provides strategic direction
- Ensures that the objectives are achieved
- Ascertains whether **risk** is being managed appropriately
- Verifies that the organization's resources are being used responsibly

GRC

Governance

Risk Management

Compliance

It is the process by which the organization manages risks to acceptable levels. These risks may include investment risk, physical risk, and cyber risk.

GRC

It is the act of adhering to mandated requirements defined by laws and regulations.

Roles of Cybersecurity

Cybersecurity Roles

The success of a cybersecurity role is ultimately the responsibility of the board of directors.

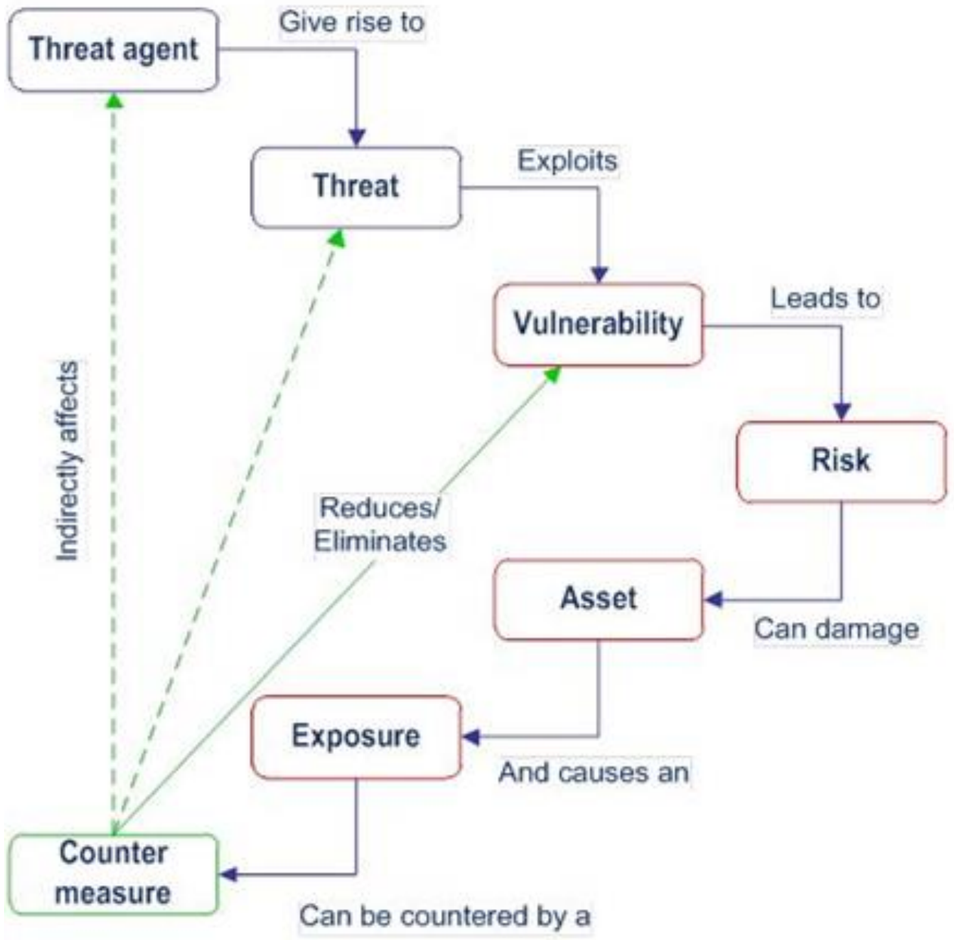
Approaches to Cybersecurity

Compliance-based security

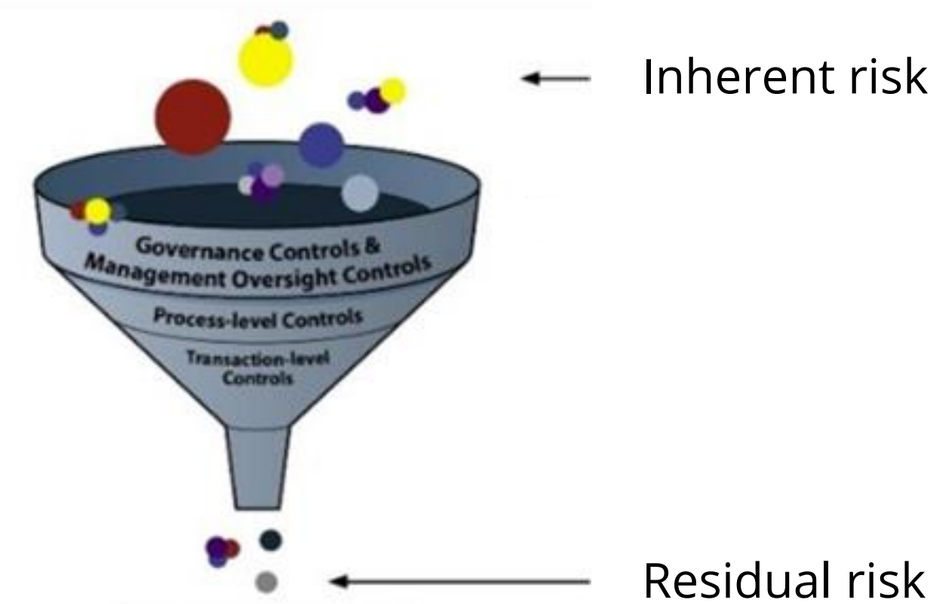
Risk-based security

Ad-hoc approach

Cybersecurity: Key Terms



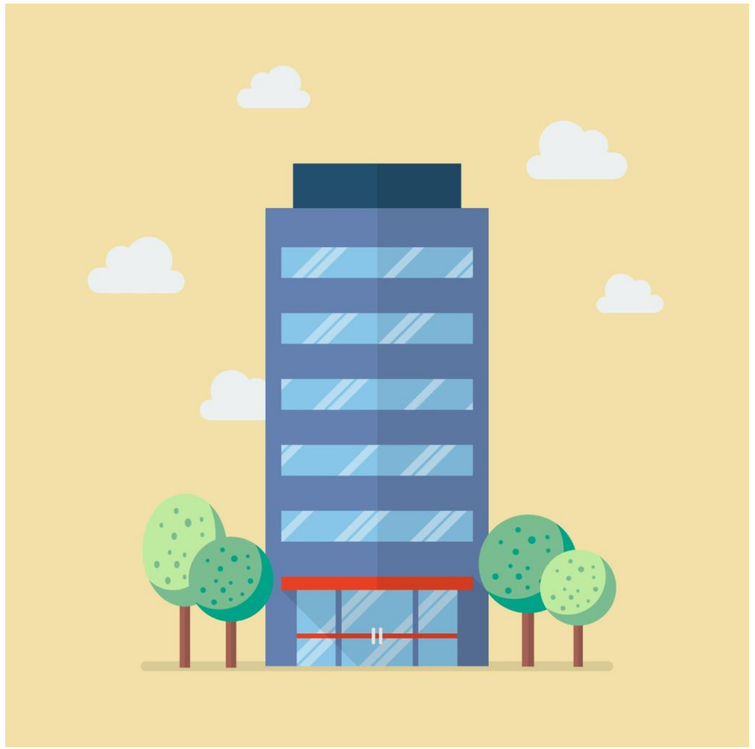
Cybersecurity: Key Terms



Inherent risk

Residual risk

Illustration: Basics of Cybersecurity



Threat Actors, Attacks, and Mitigation

Threat Actor

A threat actor or malicious actor is a person or entity that is responsible for an event or incident that impacts or has the potential to impact the safety or security of another entity.

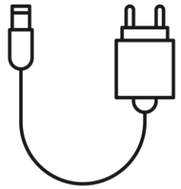
Threat Actor Categories

Threats to a System

Main threats to an organization should be considered.

Natural environmental threats

Supply system threats



Man-made threats

Sociopolitical threats

Malware

Malware is any software that is intentionally designed to cause damage to a computer, server, client, or computer network.

Types of Malware

- Worms
- Viruses
- Trojans
- Spyware
- Adware
- Rootkit
- Backdoor
- Logic bombs
- Ransomware

Worms

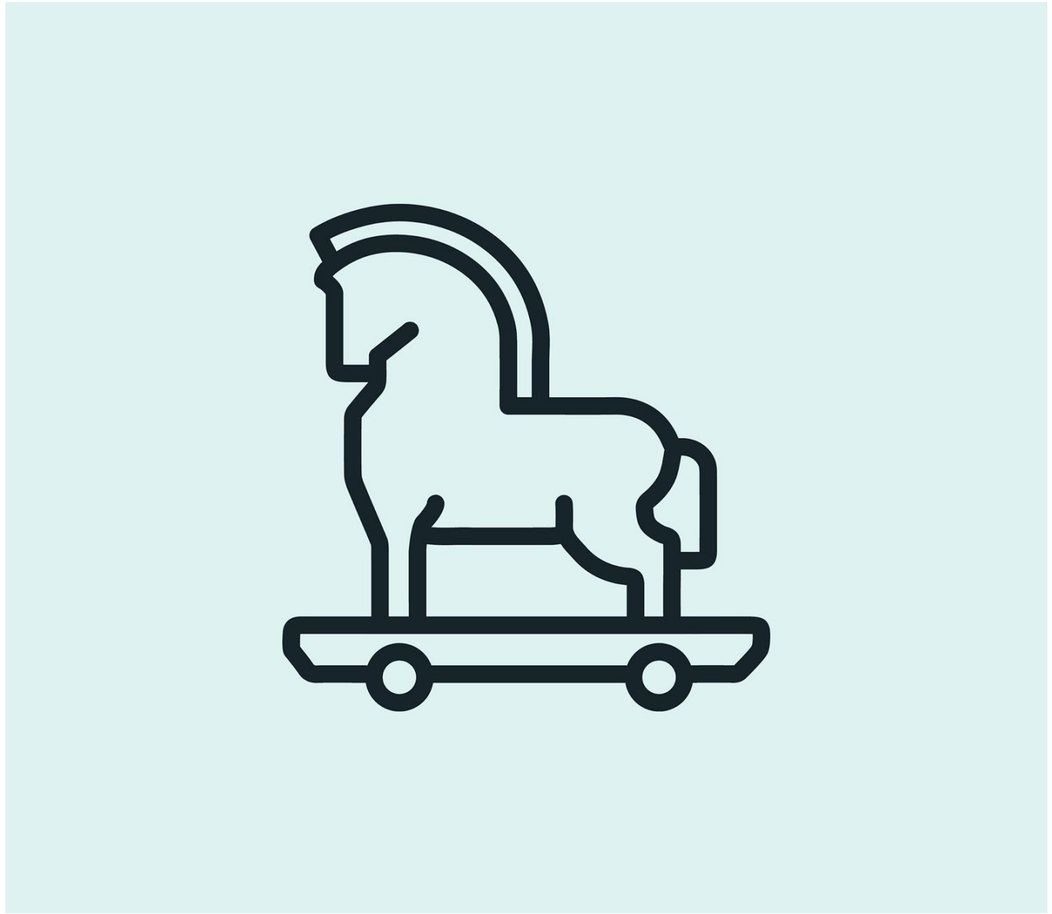
Worms are self-replicating codes designed to penetrate computer systems.

Virus

Virus is a malicious code that replicates by attaching to an executable code.

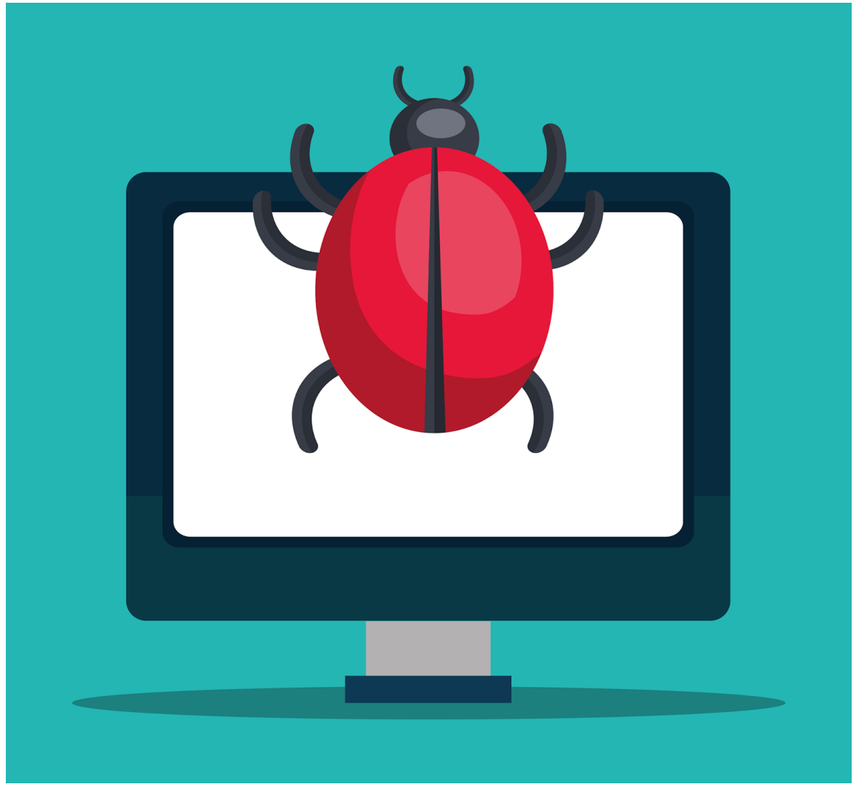
Trojans

Trojans are programs that claim to perform one function but does another, typically malicious.



Spyware

Spyware is a software aimed to steal personal or organizational information.

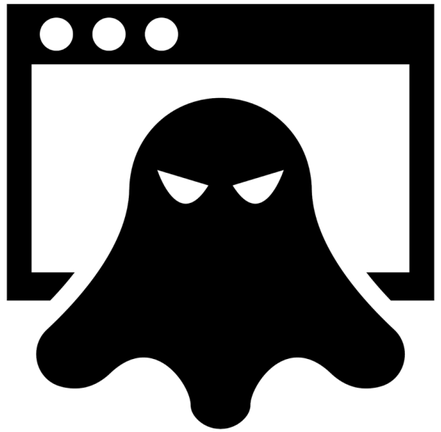


Adware

Adware is a software that displays endless ads and pop-up windows.

Rootkit

Rootkits are designed to modify the operating systems' operations to facilitate non-standard functionality.



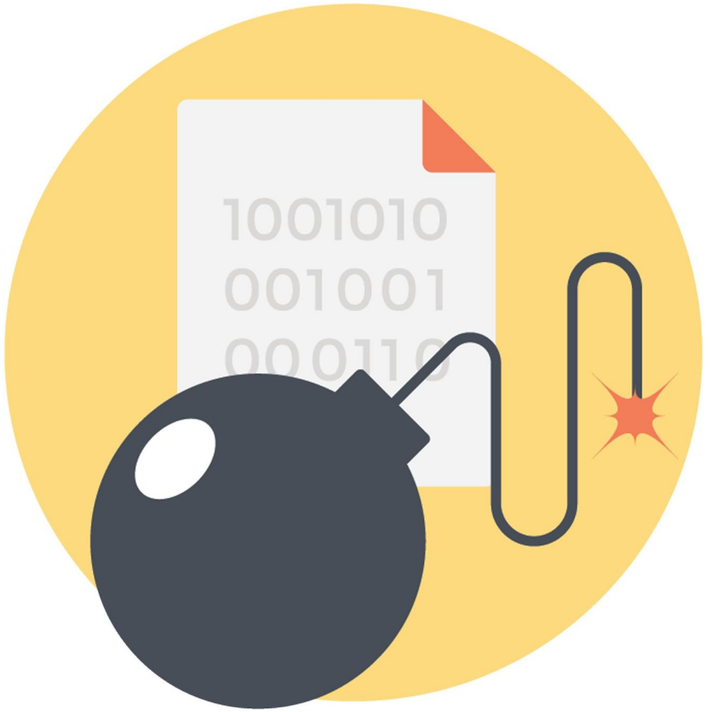
Rootkit

Backdoor

Backdoor provides the attacker with unauthorized remote access to a system by exploiting security vulnerabilities.

Logic Bombs

Logic bombs infect a system and lie dormant until they are triggered by a specific condition.



Ransomware

Ransomware attempts to extort money from the user by infecting and taking control of a victim's machine.

Malware Attacks

Kovter

WannaCry

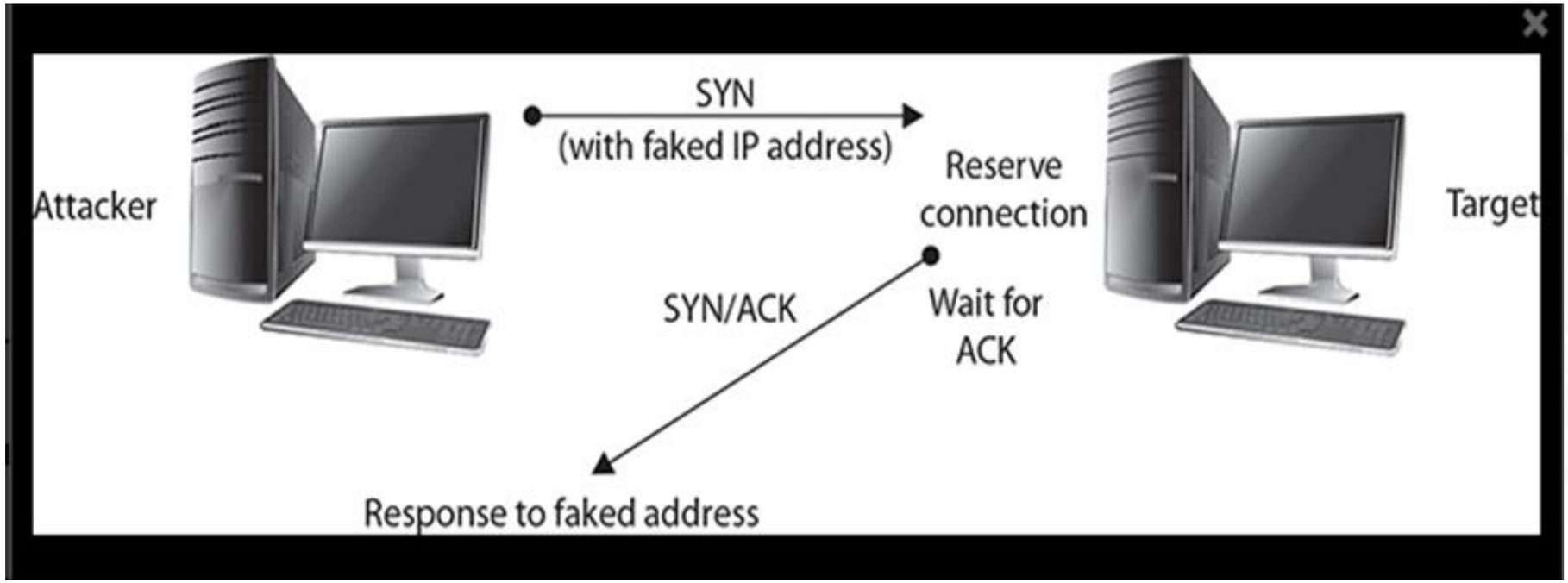
Zeus or Zbot

Ghost

Mirai

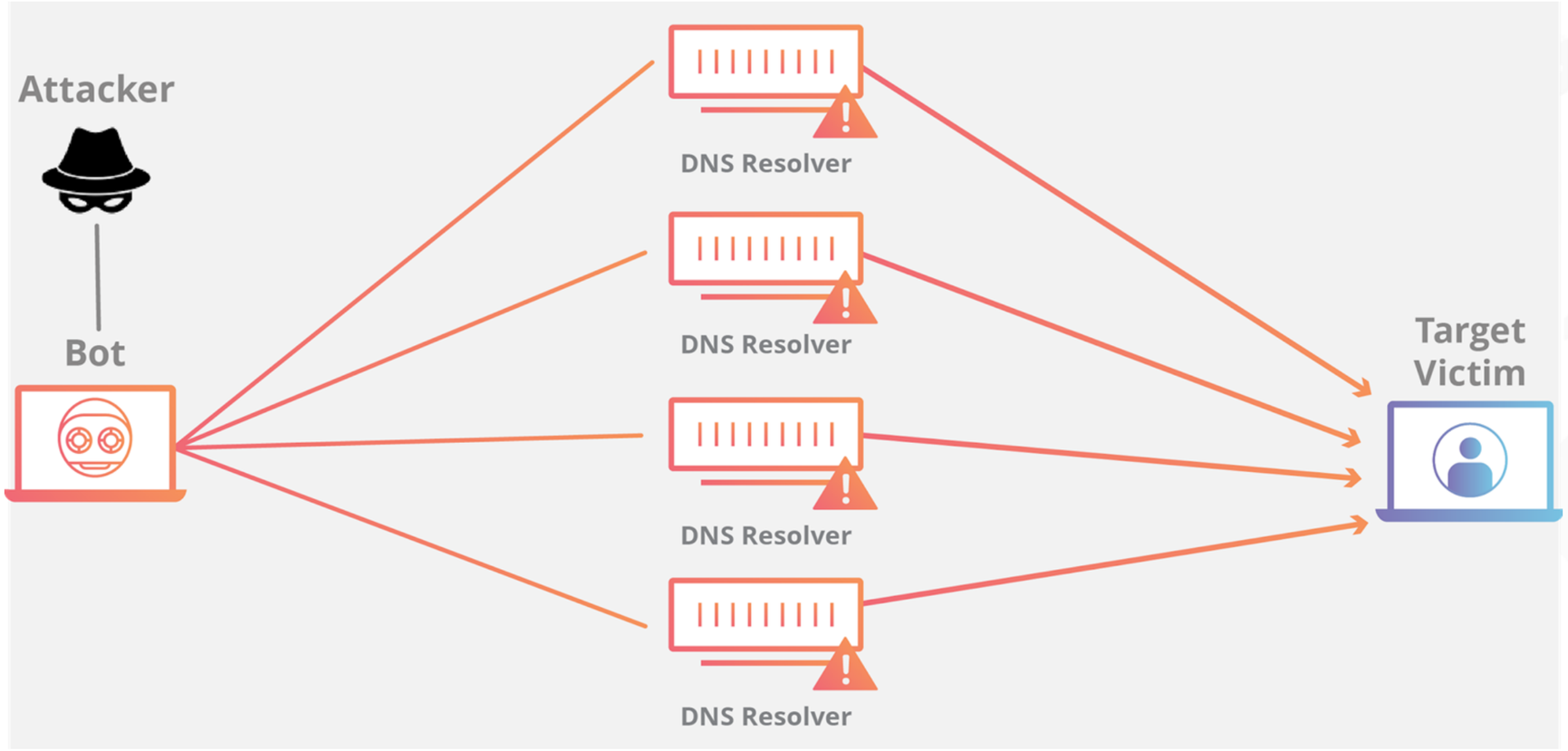
Denial-of-Service Attack

The purpose of DoS is to prevent access to the target system.



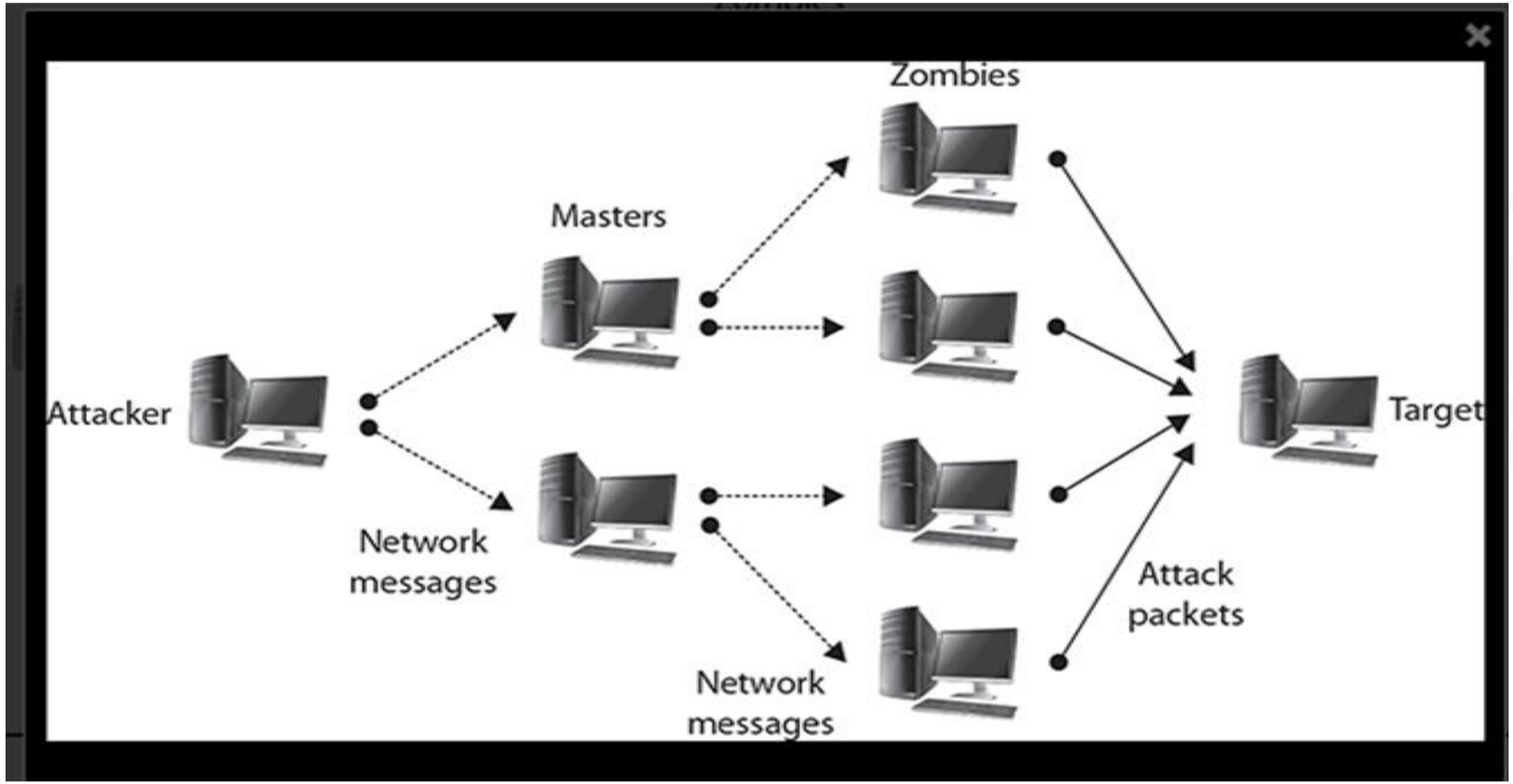
Distributed Denial-of-Service

It is a denial-of-service attack employing multiple attacking systems.



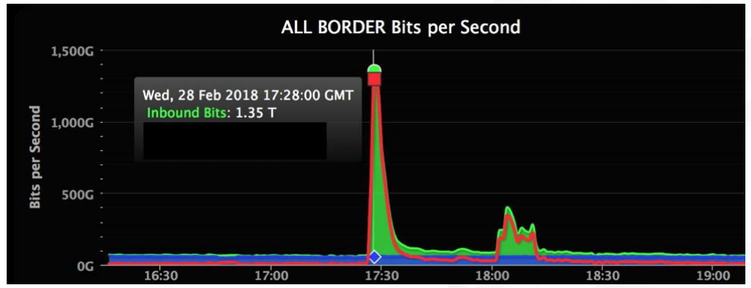
Distributed Denial-of-Service

The goal of DDoS is to prevent access to a specific system.



DoS/DDoS Attacks

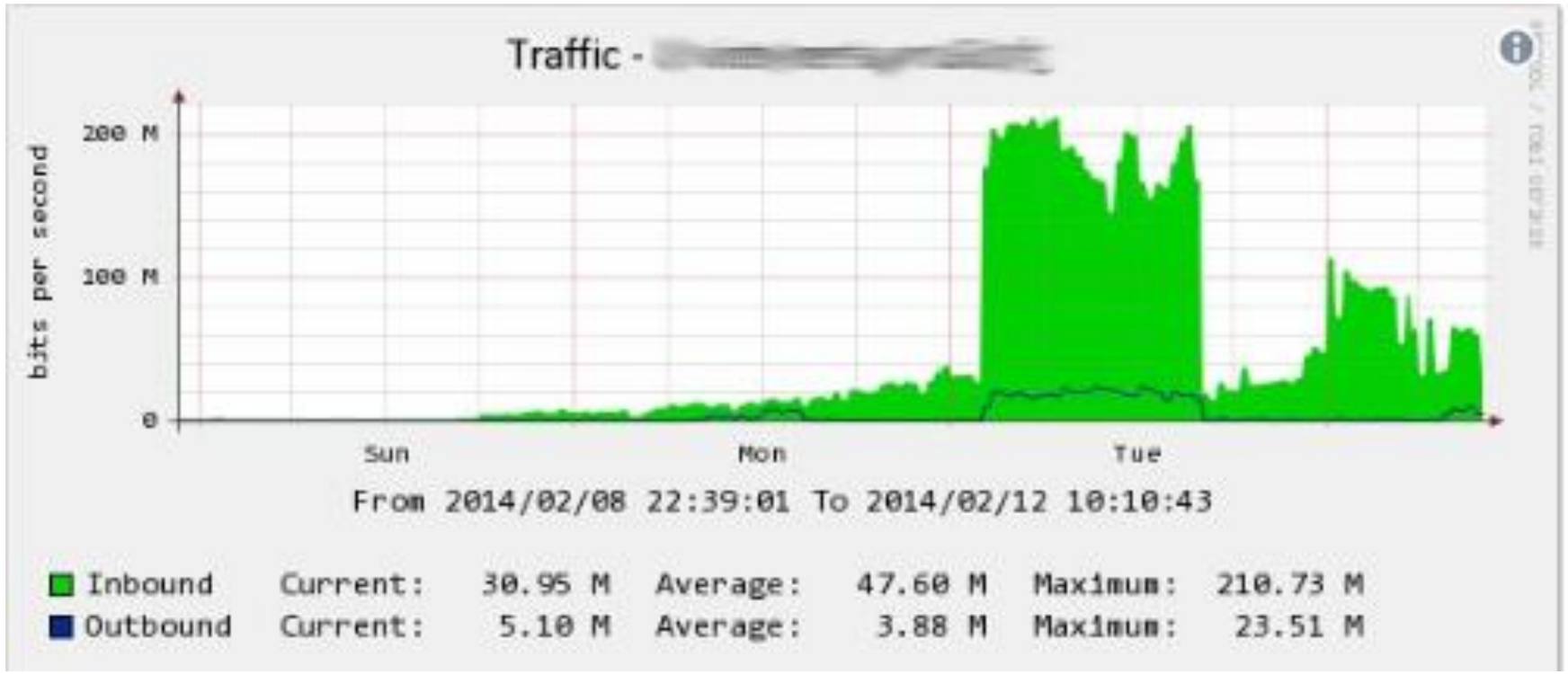
GitHub: 1.35 Tbps



GitHub was hit with 1.35 terabits per second of traffic.

DoS/DDoS Attacks

Cloudflare: 400 Gbps



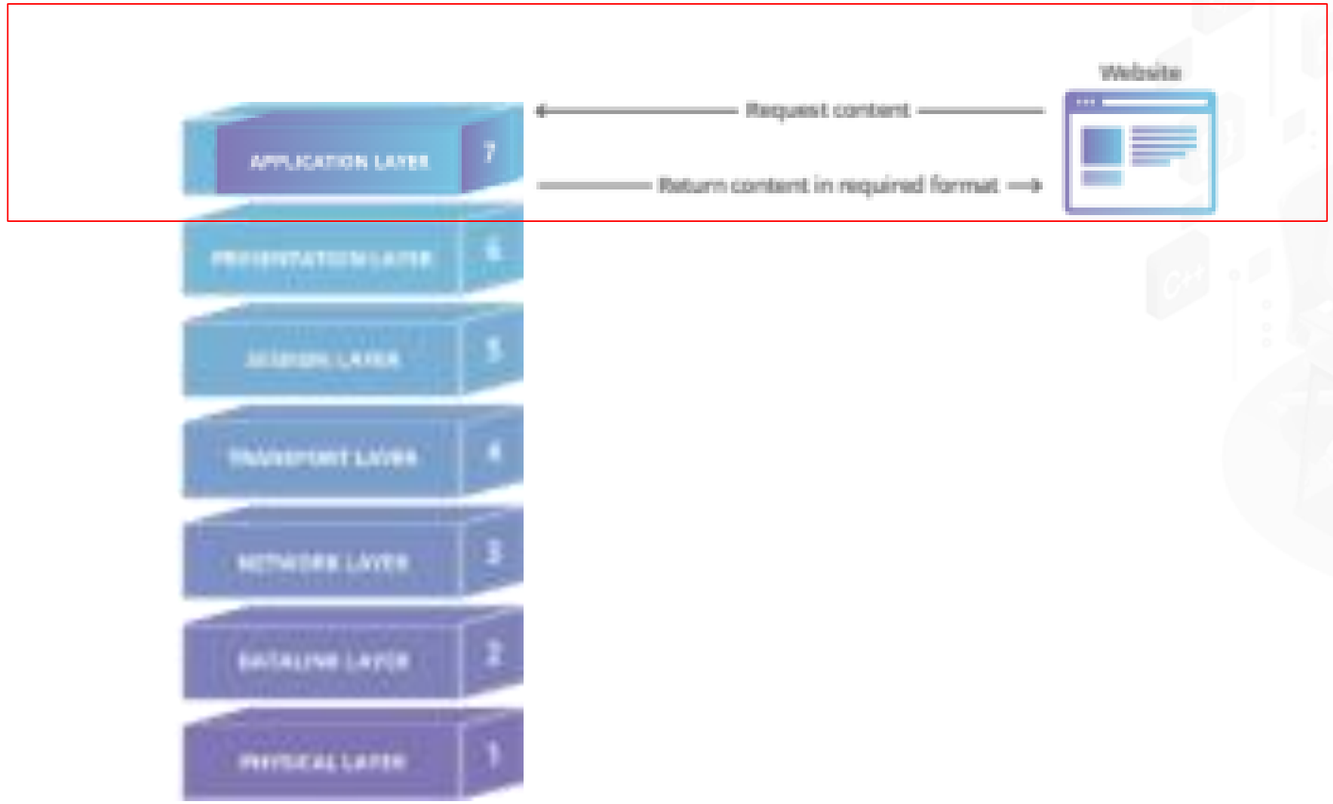
The attack was directed at a single computer with vulnerability.

Application Layer Attacks

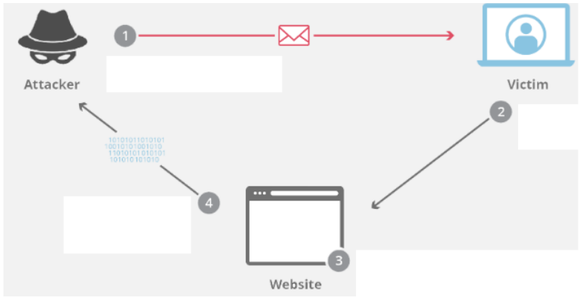
They target computers by causing a fault in the operating system or applications.

Application Layer Attacks

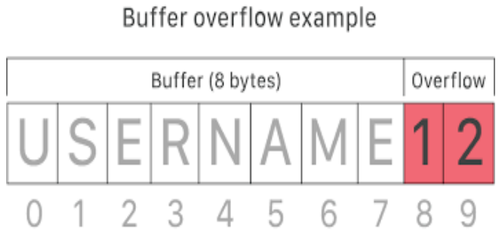
They refer to a type of malicious behavior designed to target the top layer in the OSI model.



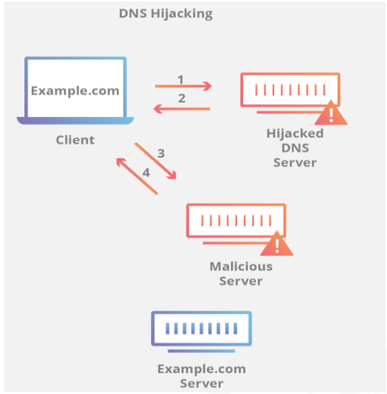
Application Layer Attacks



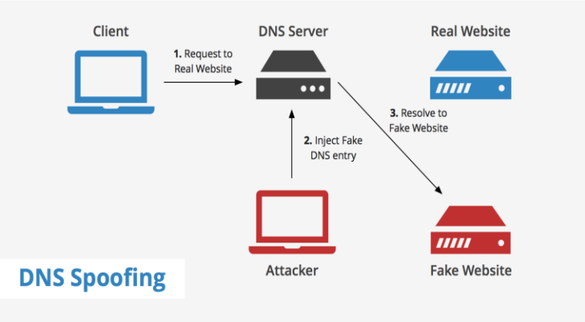
Cross-site scripting



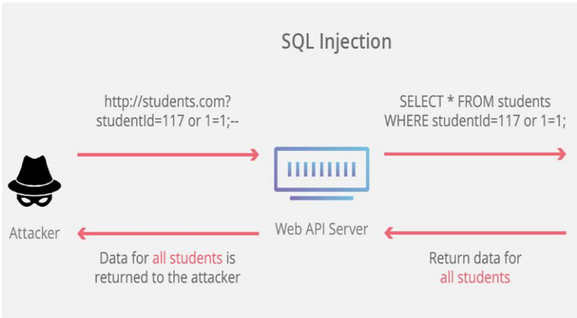
Buffer overflow



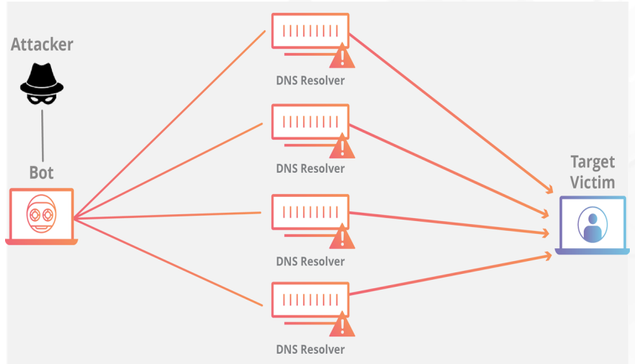
Domain hijacking



DNS spoofing



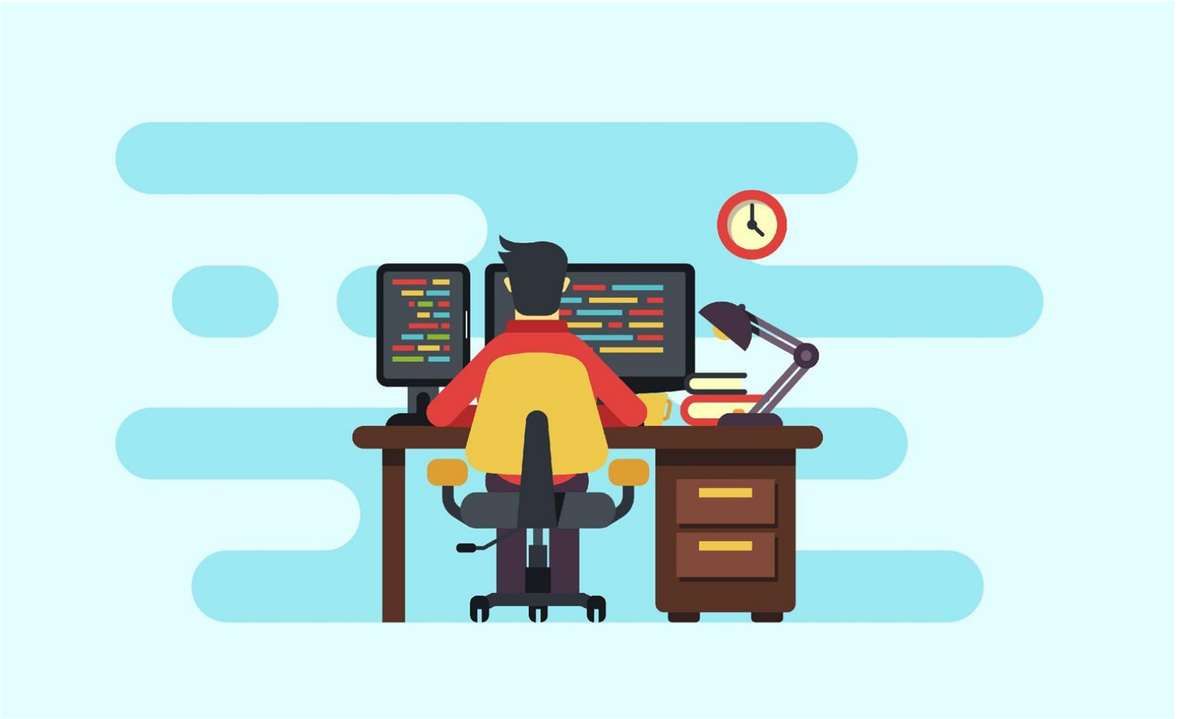
SQL injection



DoS/DDoS

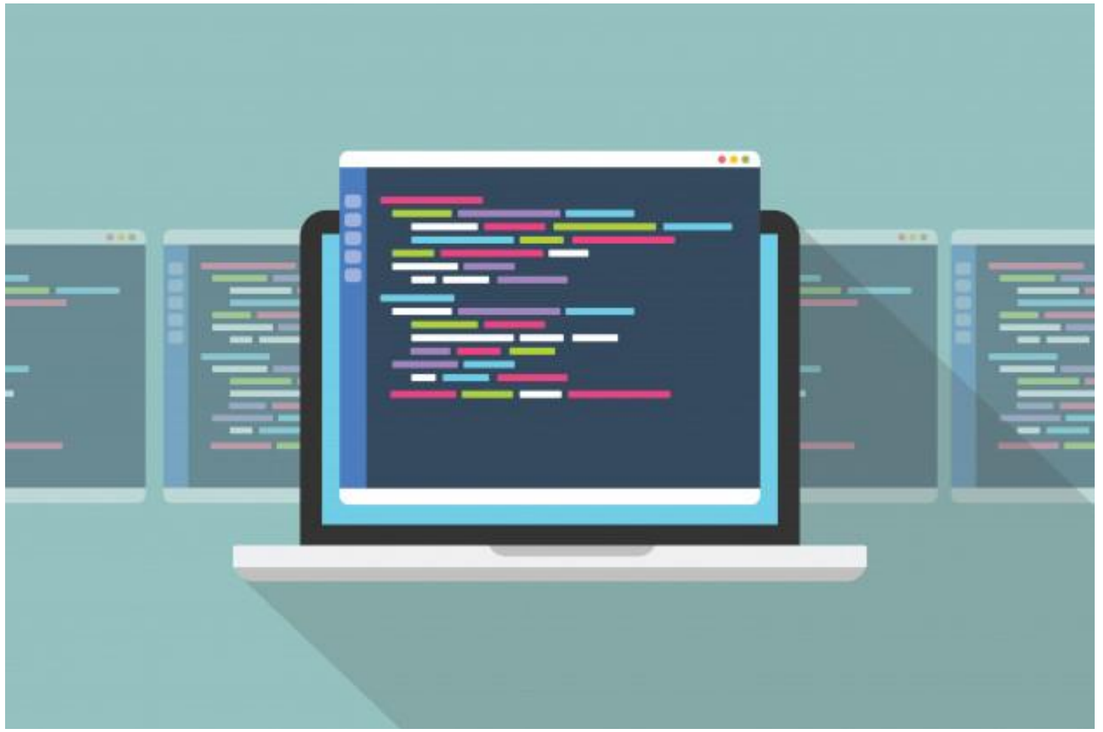
Software Codes and Security

Programmers are responsible to write safe and high quality codes.



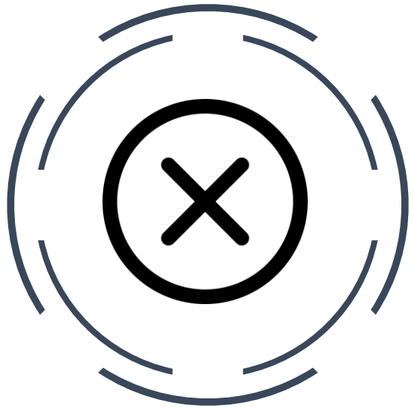
Software Codes and Security

Source codes are statements written using a computer programming language.

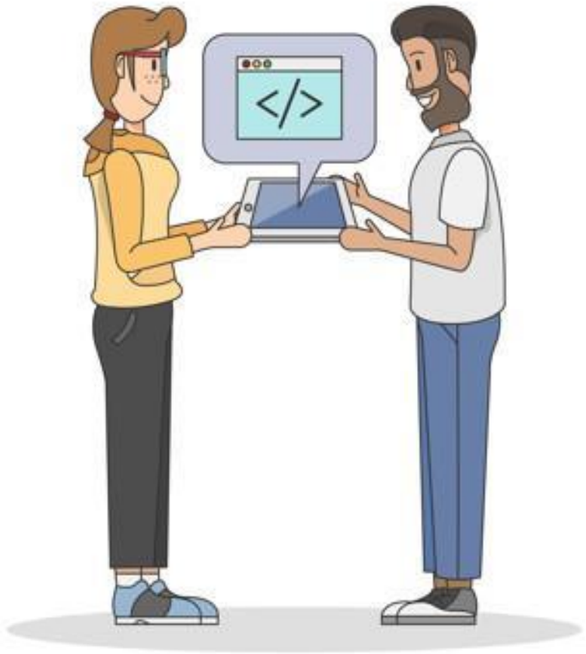


Software Codes and Security

Code review is a systematic examination or peer review of source code.

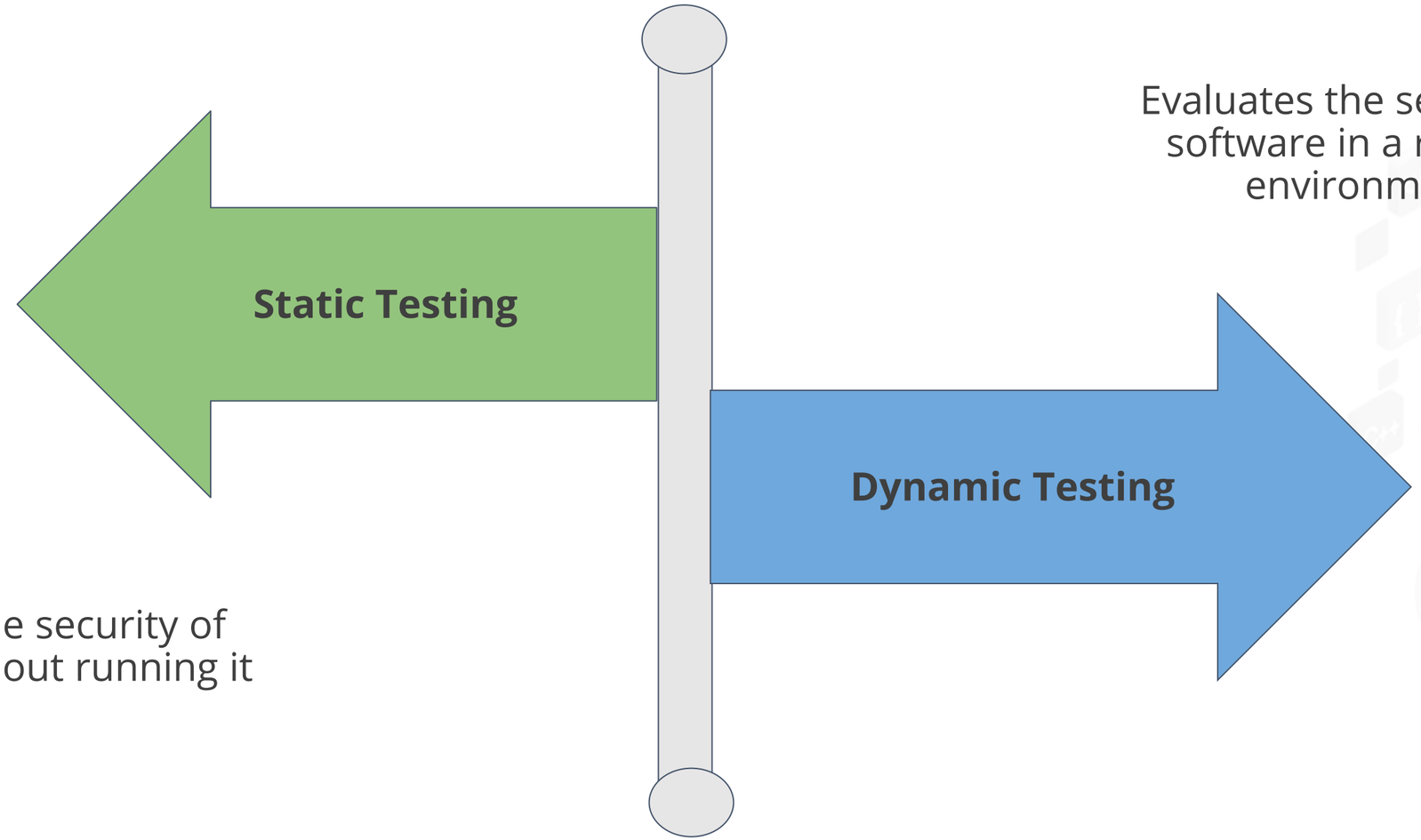


Find mistakes



Improve software quality

Software Testing Methods

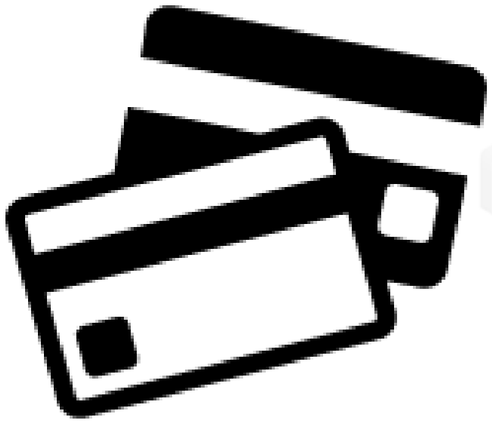


Evaluates the security of software without running it

Evaluates the security of software in a runtime environment

Software Testing Methods

In March 2018, hackers hit Saks Fifth Avenue and Lord & Taylor, stealing debit and credit cards.



5 million records breached

Software Testing Methods

In May 2018, the concert and sporting event ticketing website, **ticketfly** was vandalized, taken down, and disrupted for a week.

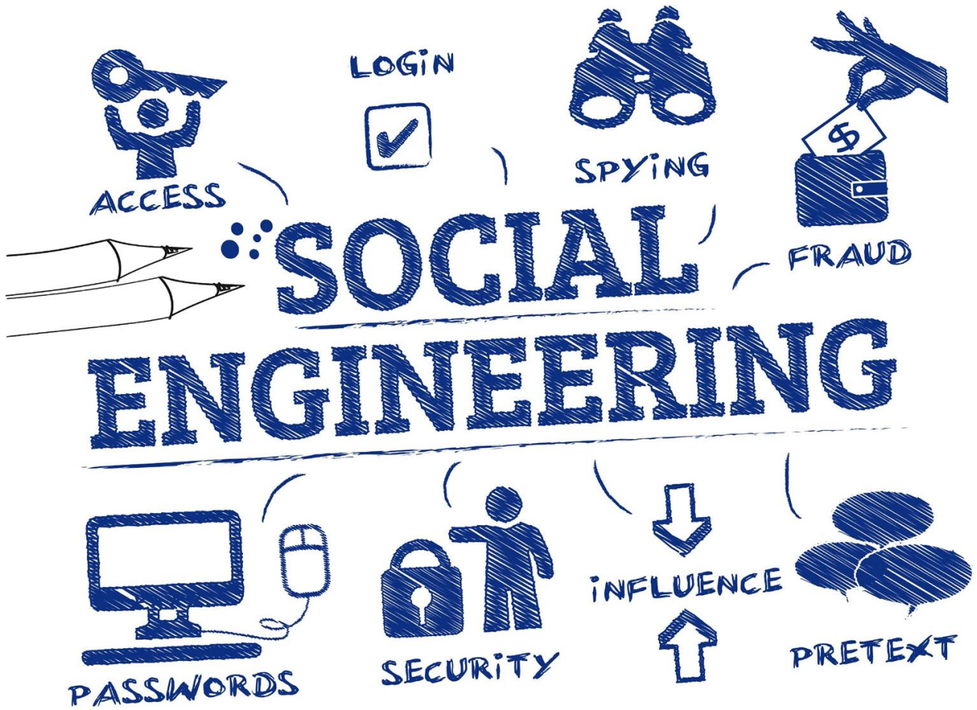
Security Attacks

In August 2018, Russian hackers made millions selling credit card details stolen from almost 245,000 British Airways customers.

BRITISH AIRWAYS

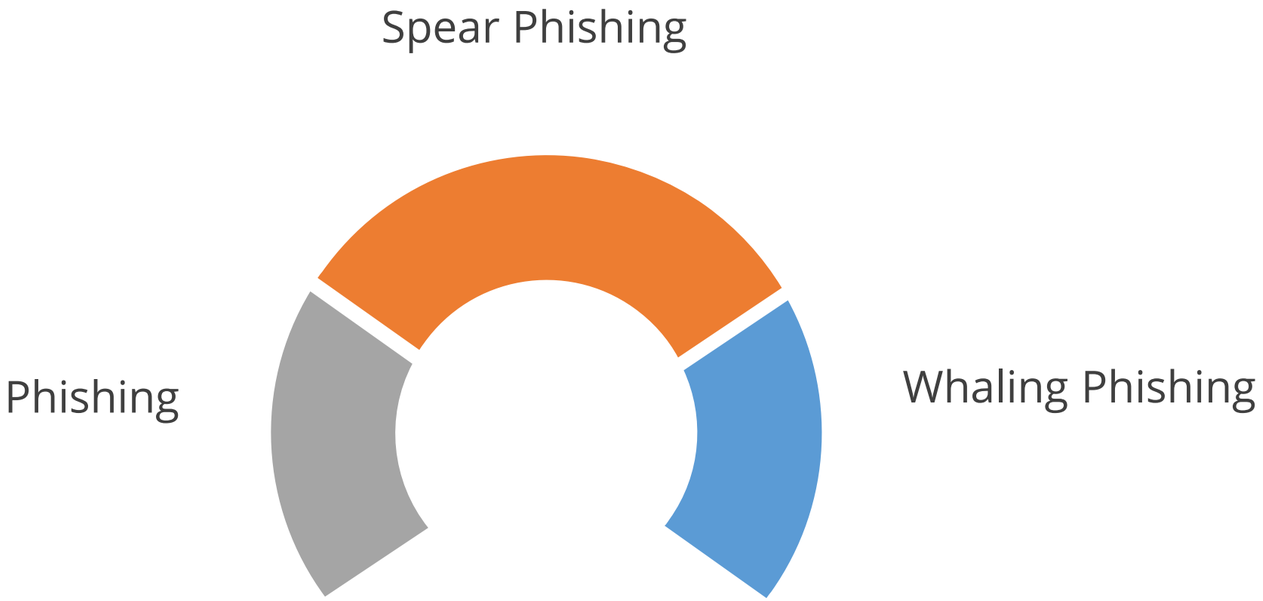
Social Engineering

It is the art of manipulating people, so they give up their confidential information violating the security principle.



Social Engineering Attack Categories

There are several attack categories of social engineering.



Social Engineering Attack Categories

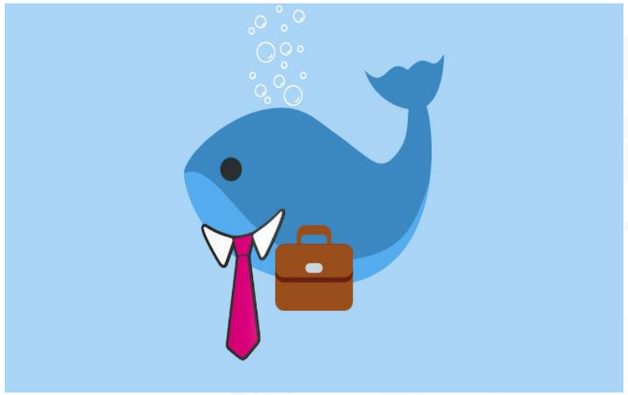
Phishing

It is a fraudulent attempt to obtain sensitive information.

Spear Phishing

It is targeted to a specific group or an individual.

Whaling Phishing



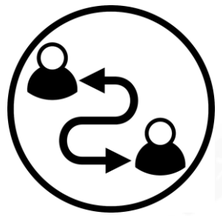
It targets wealthy and prominent individuals.

Social Engineering Attack: Ethereum Classic

In 2017, Ethereum Classic website was hacked resulting in the loss of thousands of dollars in cryptocurrency.

Social Engineering Attack: Ethereum Classic

Impersonated Ethereum owner



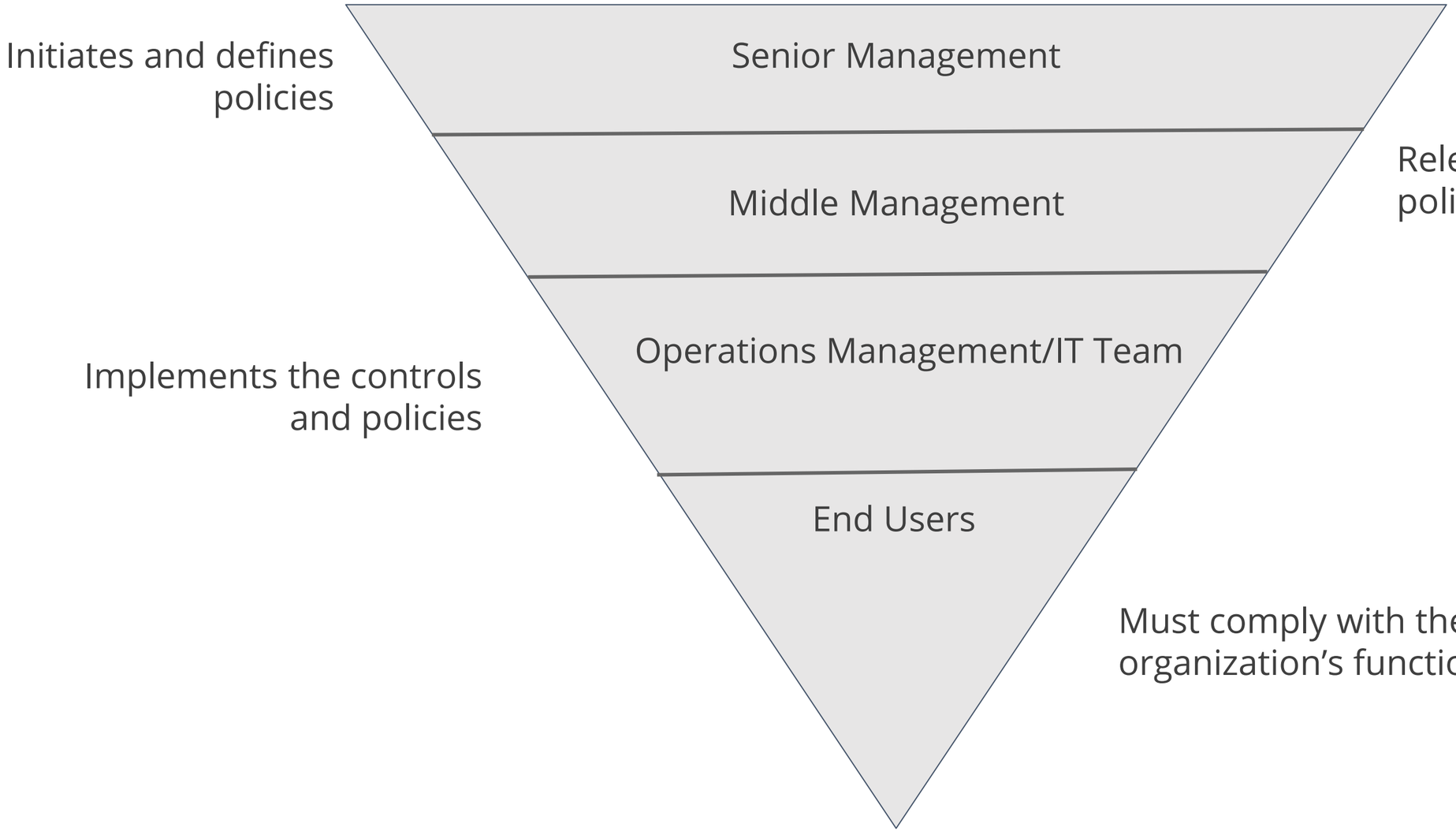
Redirected the domain to their server

Gained access to domain registry

Extracted cryptocurrency from the victims

Security Policies and Procedures

Security Management Plan



Types of Security Management Plan

Strategic Plan

Tactical Plan

Operational Plan

Types of Security Management Plan

Strategic Plan

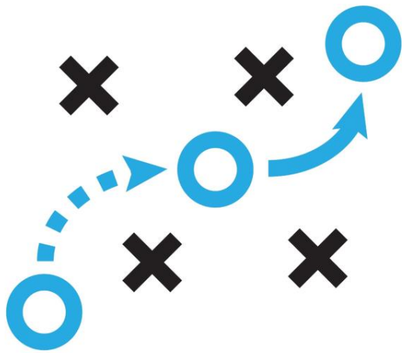
Tactical Plan

Operational Plan

- Is a long-term plan
- Defines security posture
- Is valid for five years and is renewed annually
- Helps understand security functions
- Helps in risk assessment

Types of Security Management Plan

Strategic Plan



Tactical Plan

- Is a mid-term plan
- Provides detailed goals
- Is updated every year or two
- Is technology oriented

Operational Plan

Types of Security Management Plan

Strategic Plan

Tactical Plan

Operational Plan

- Is a short-term plan
- Is highly detailed
- Is updated monthly or quarterly
- Spells out how to accomplish goals

Security Policy

- Is a strategic plan
- Defines the scope of security
- Outlines security objectives and framework
- Identifies the functional areas
- Outlines security goals and practices
- Assigns responsibilities and requirements
- Defines risk levels

Types of Security Policy

Focuses on issues relevant to every aspect of the organization

Organizational policy

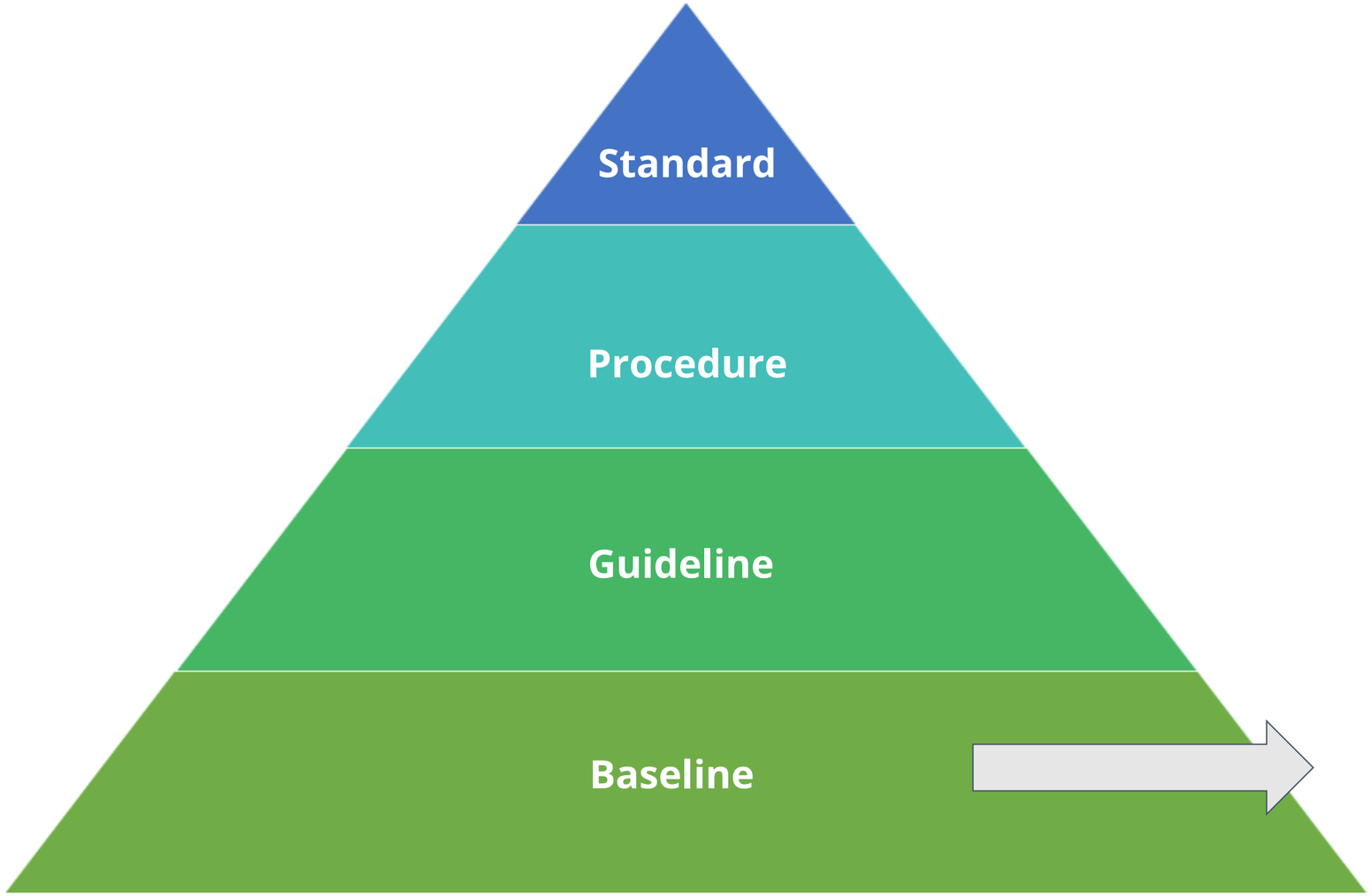
Issue-specific policy

System-specific policy

Focuses on a specific service, department, or function

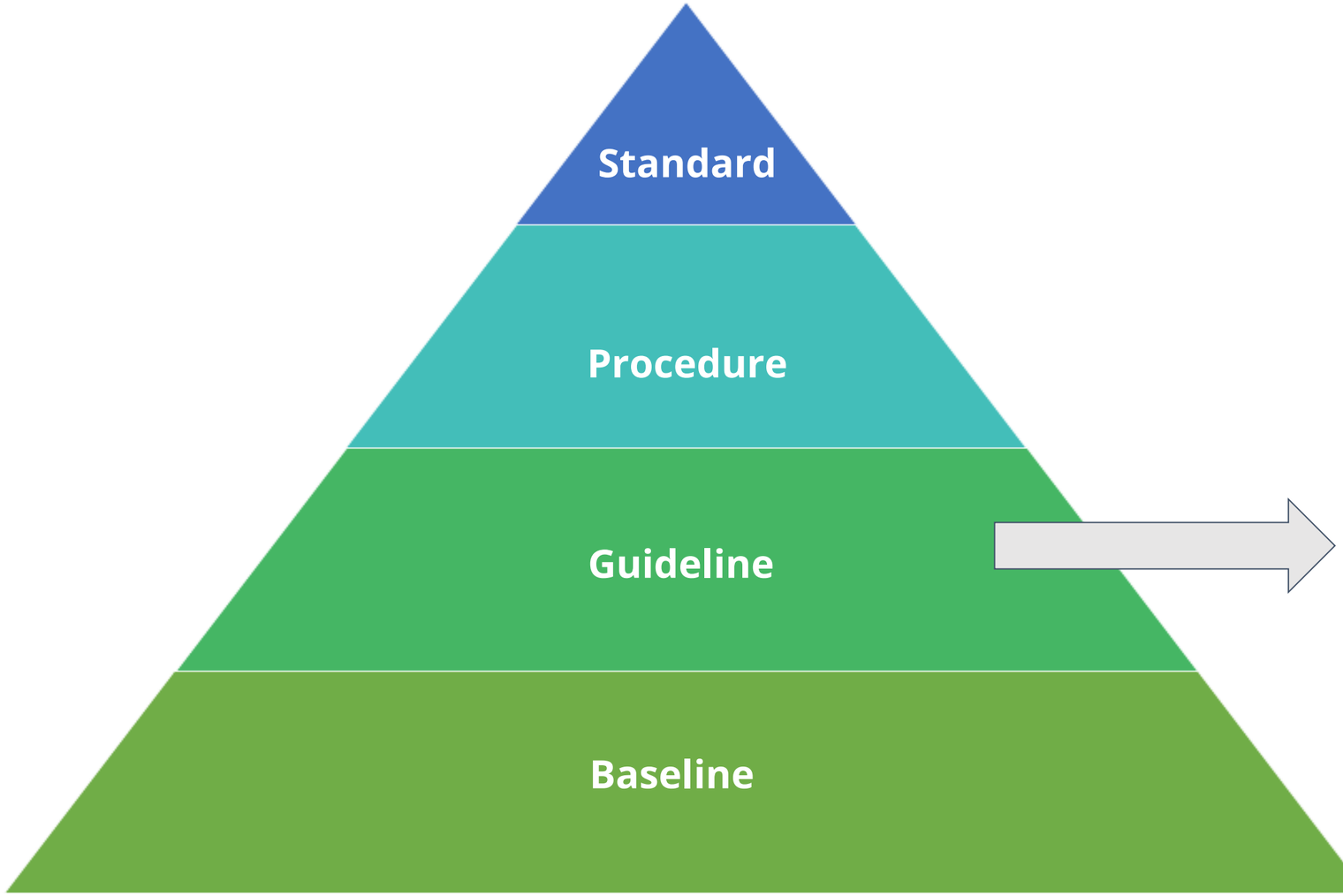
Focuses on individual systems

Security Policy Framework



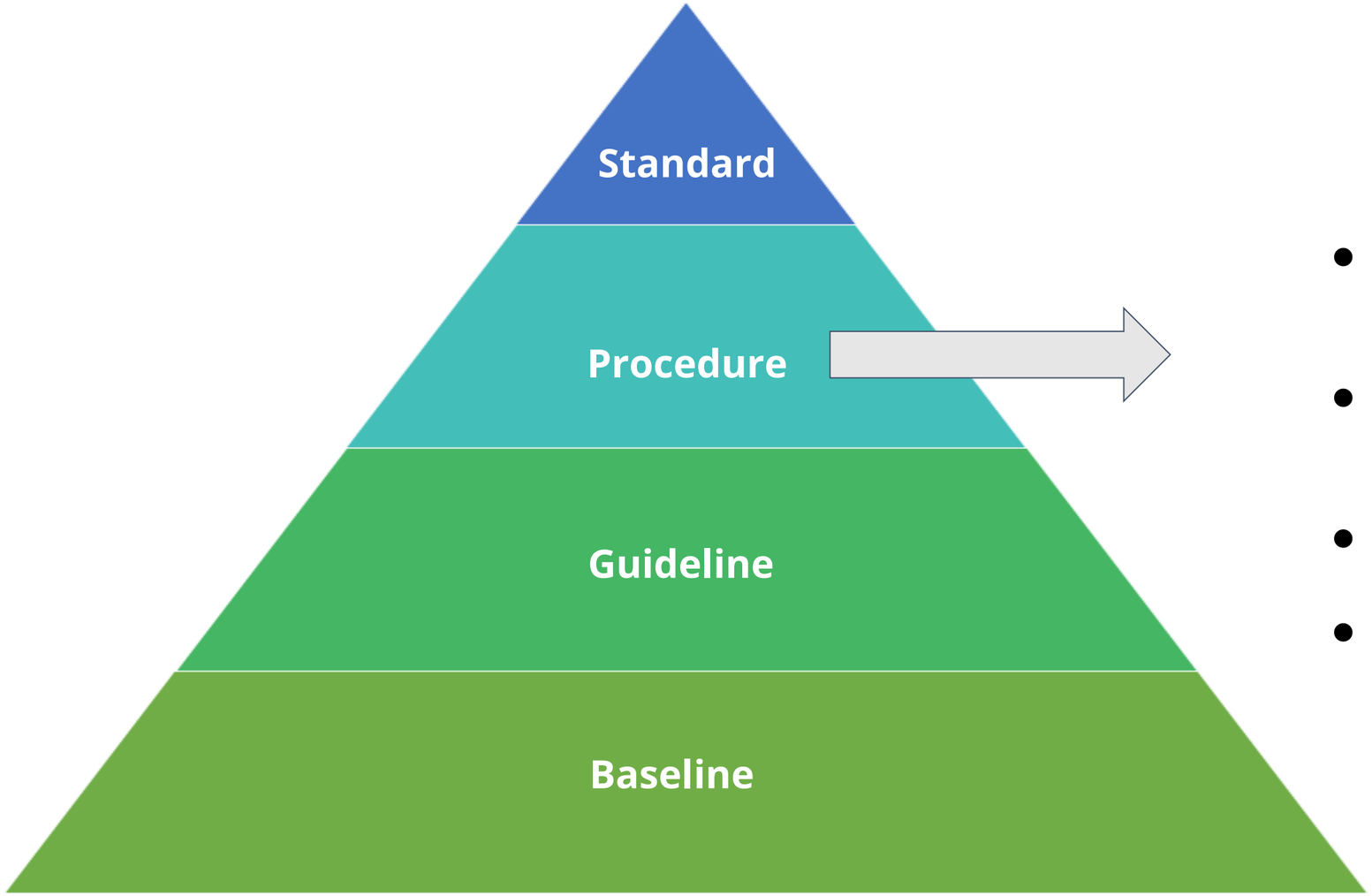
- Defines the minimum level of security
- Is system specific
- Establishes the common secure state

Security Policy Framework



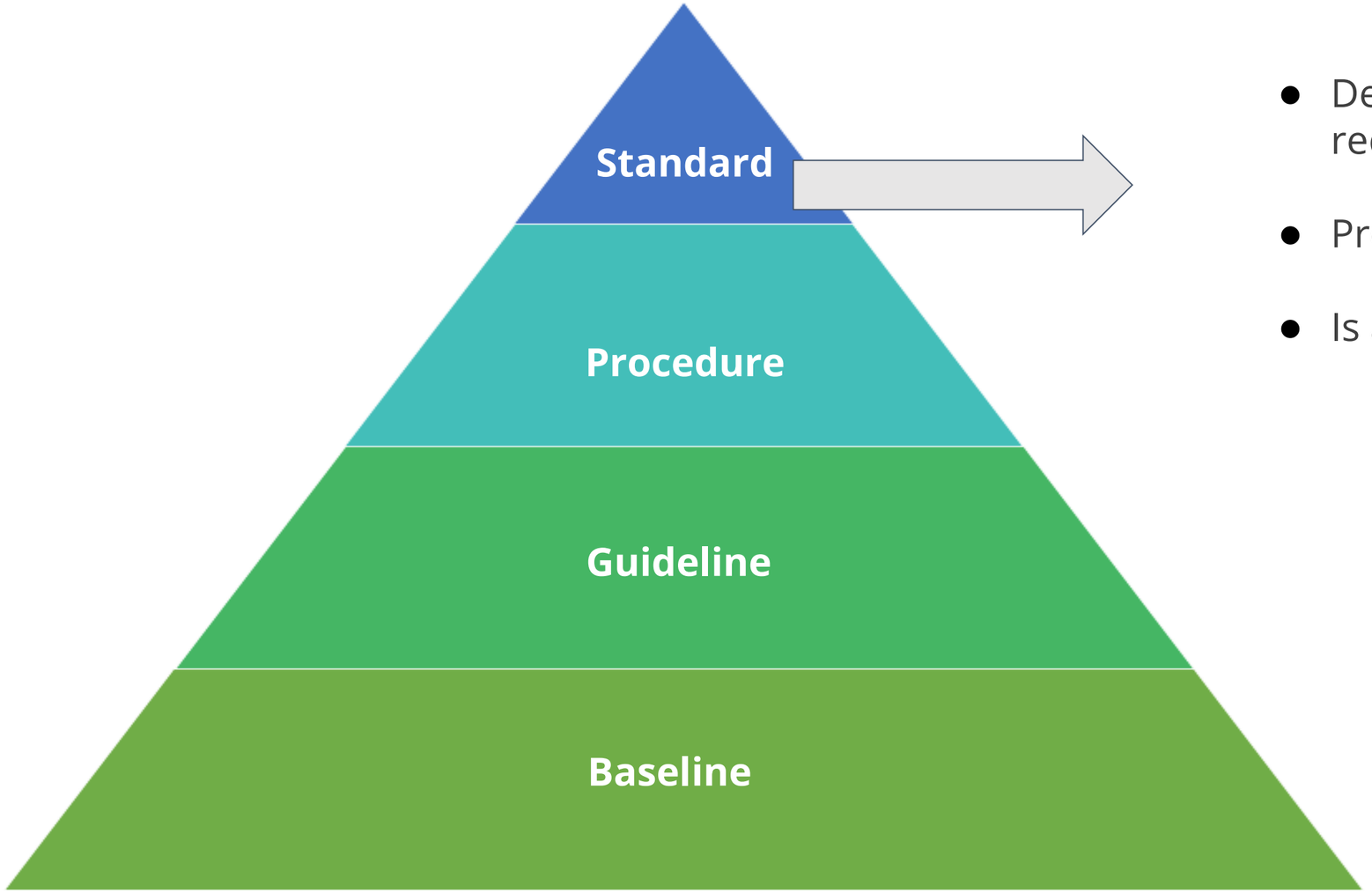
- Offers recommendations on implementation
- Serves as an operating guide
- Is customized for each unique system

Security Policy Framework



- Is the final element of formalized security policy structure
- Describes actions for implementing the security mandates
- Is system and software specific
- Ensures integrity of the business process

Security Policy Framework



- Defines the compulsory requirements
- Provides a course of action
- Is a tactical document

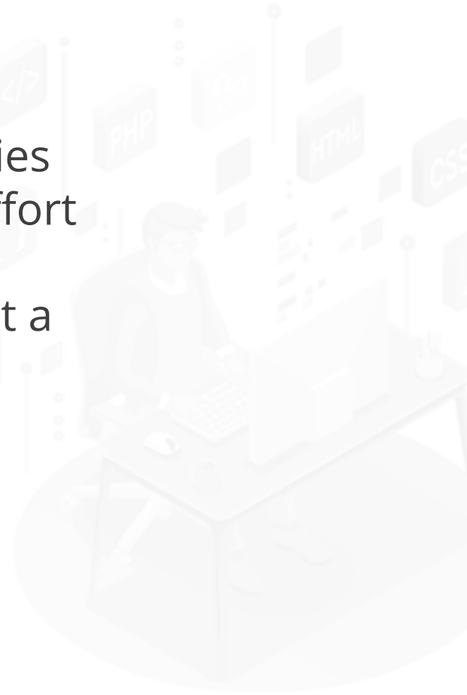
Due Care and Due Diligence

Due Care

- Reasonable care is taken in protecting the organization
- Pertains to the legal duty of the organization
- Lack of due care is considered negligence

Due Diligence

- Is about practicing the activities that maintain the due care effort
- Pertains to best practices that a company should follow
- Might not be legally liable



Cybersecurity Mitigation Methods

Information Technology Control

An IT control is a procedure or policy that provides a reasonable assurance that:

IT used by an organization is operating as intended

The organization is in compliance with laws and regulations

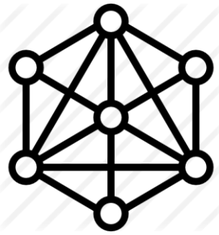
Data is reliable

Countermeasure

It is an action or method that is applied to prevent, avert, or reduce potential threats to:

Computers

Networks

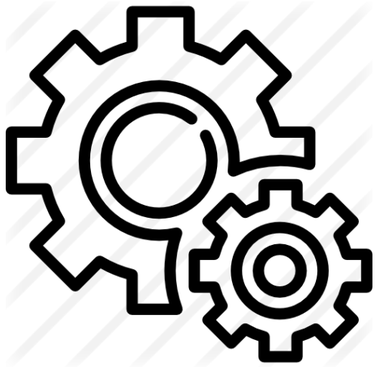


Servers

Operating systems

Information systems

Countermeasure



It helps to mitigate or reduce the potential risk.

Control Categories

Administrative controls

Technical controls

Physical controls

Administrative Controls

These are procedures and policies used to define employee actions toward sensitive information.

Technical Controls

These are hardware or software mechanisms used to protect important and confidential assets.

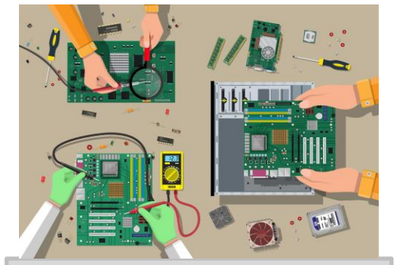
Physical Controls

These are security measures designed to deny unauthorized access.

Physical Controls

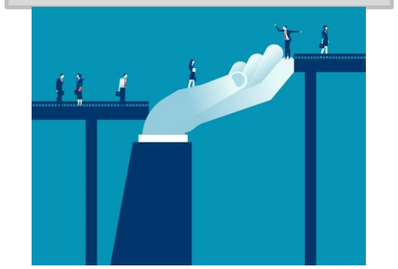
Deterrent

Preventive



Corrective

Recovery

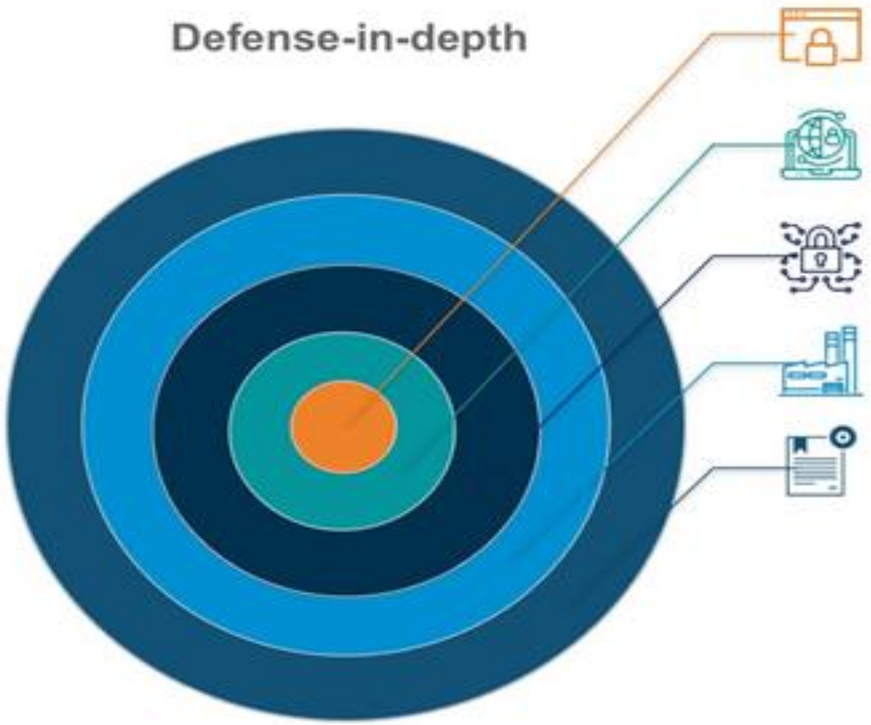


Detective

Compensating

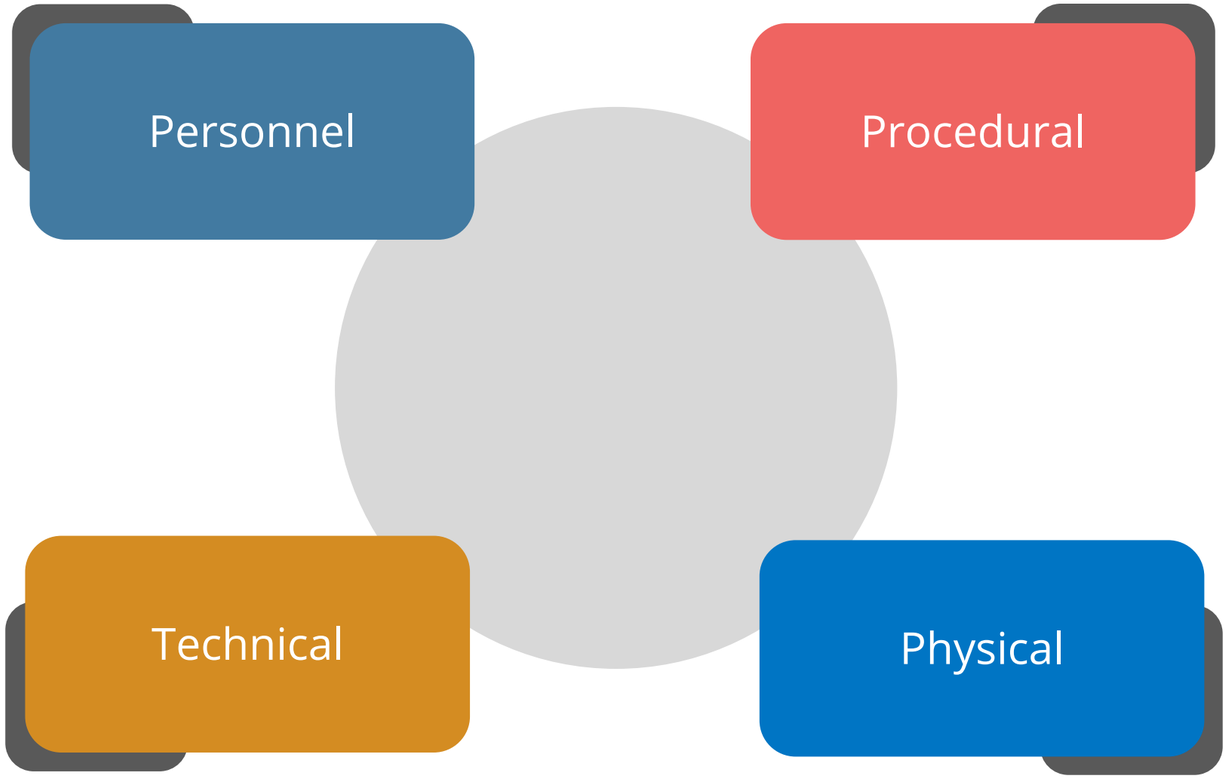
Defense in Depth or Layered Approach

It is the act of using multiple layers of security controls to protect the integrity of information.

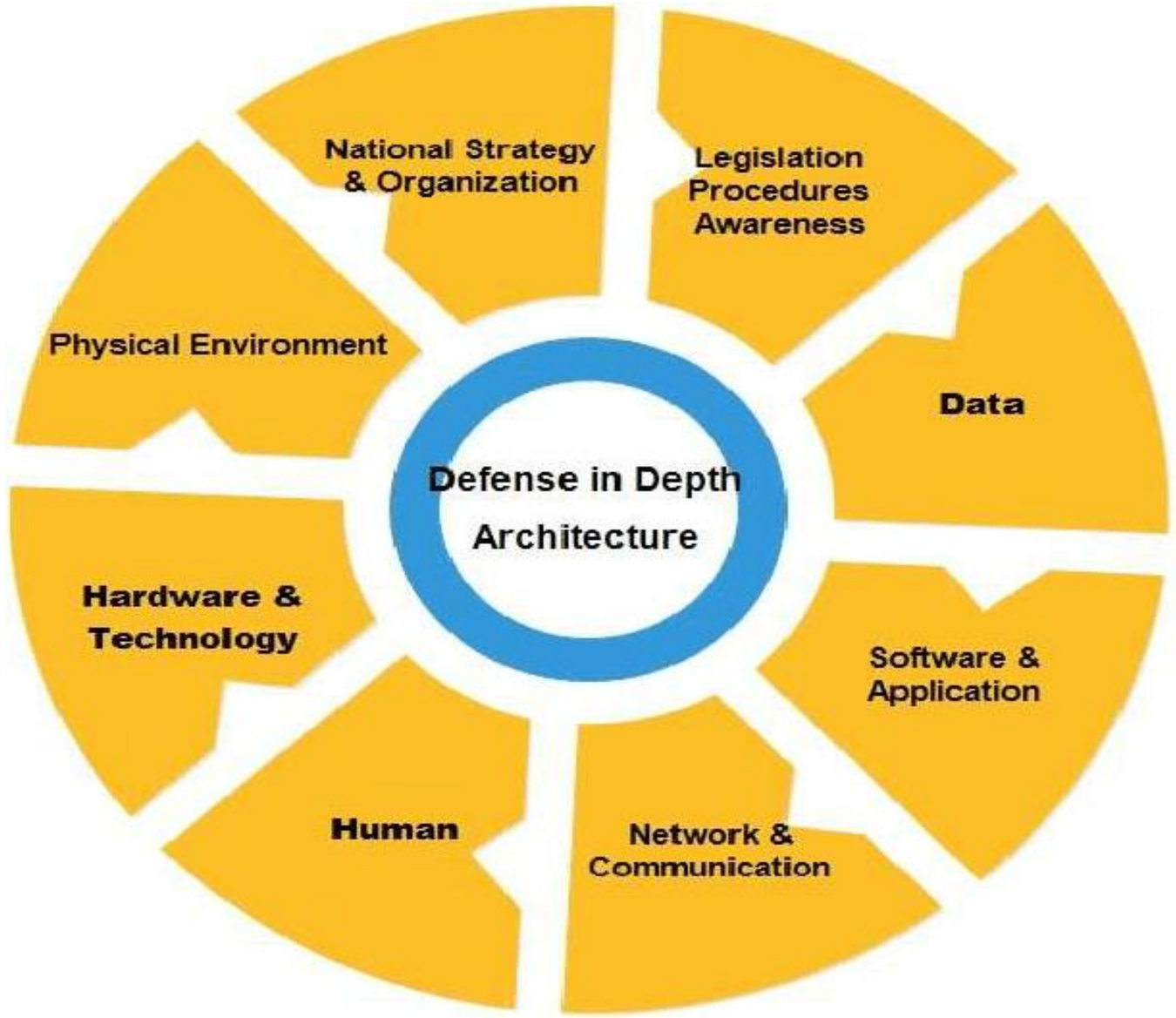


Defense in Depth or Layered Approach

Its intent is to provide increased security through intentional redundancy based on multi-layered security approach.



Defense in Depth or Layered Approach



Identity Management

It is an organizational process for identifying, authenticating, and authorizing individuals or groups of people.

Identified

Authenticated

Authorized

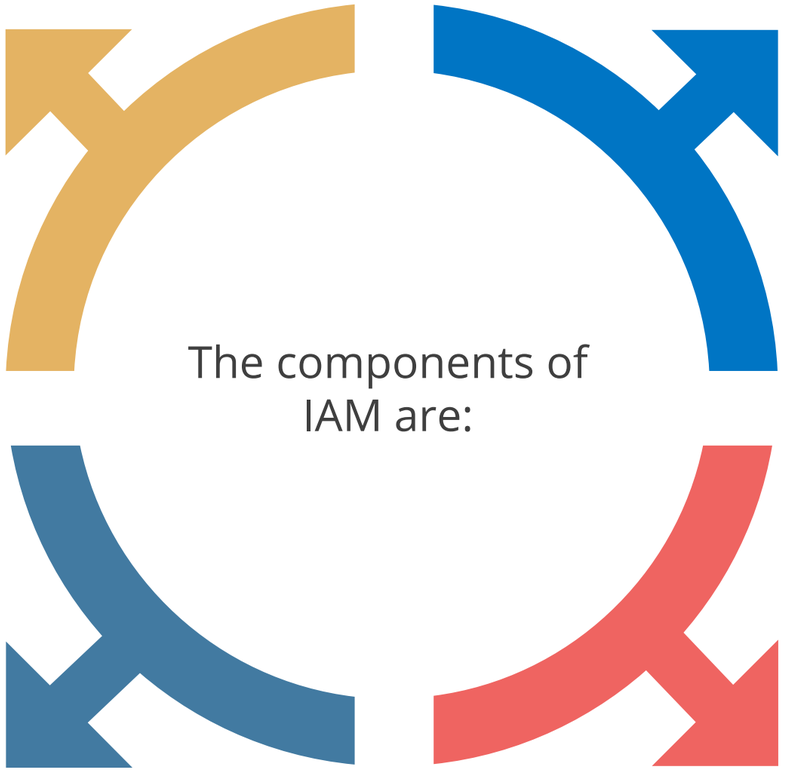
Identity Management

It enables the right users to access the right resources at the right time for the right reasons.

IAM Components

Authentication

Authorization



User Management

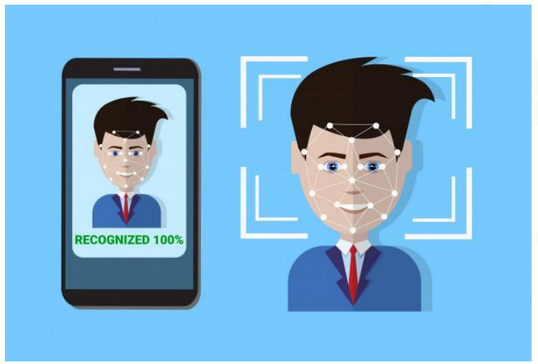
Central user repository

Identification and **Authentication**

Identification

Identify a user or an application in the system

Authentication



Prove that a user or an application is genuine

Identification and **Authentication**

Password

Something you know

Something you have

Token card

Biometric

Something you are or do

Where you are

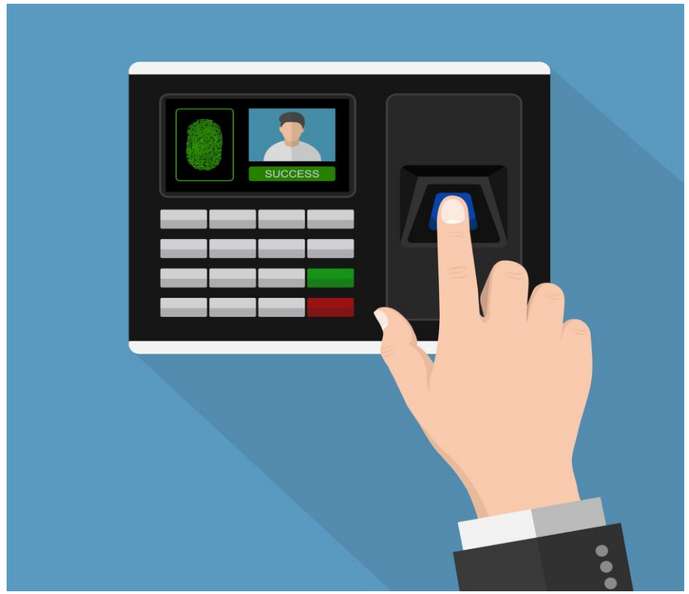
Location

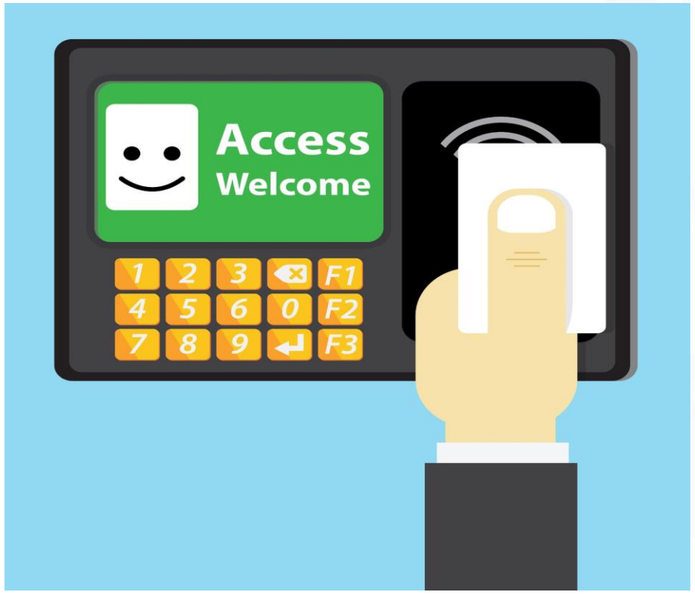
Multi-Factor Authentication

It is an authentication method where a user is granted access after presenting two or more evidences.

Two-Factor Authentication

It is a subset of multi-factor authentication, confirming that users are granted access with a combination of two different factors.





Multi-Factor Authentication

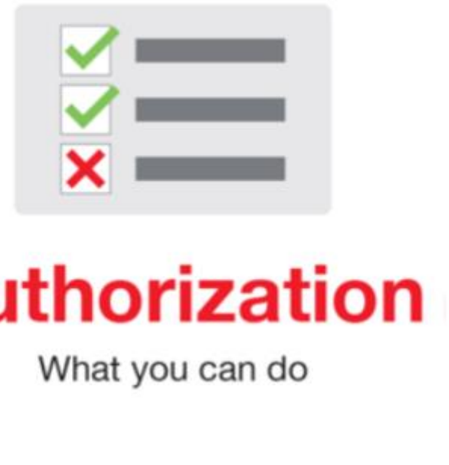
It is an authentication method where a user is granted access after presenting two or more evidences.

Authorization

It is the process of determining what types of activities, resources, or services a user is permitted.

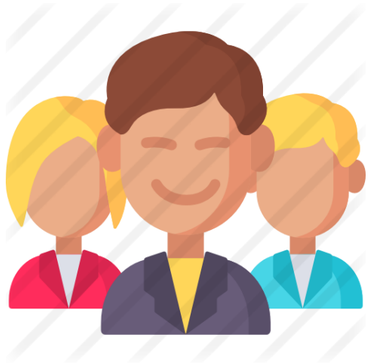
Authorization

A user may be authorized for different types of activity once authenticated.



Accountability

It is the traceability of actions performed on a system to a specific system entity.



Accountability

User identification and authentication support accountability

User ID and password destroy accountability

Auditing

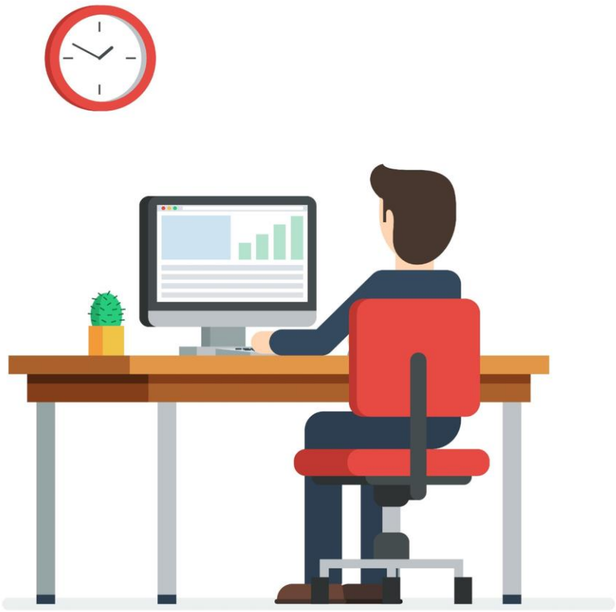
It is a manual or a systematic measurable technical assessment of a system or application.

- Interviewing staff
- Reviewing applications and OS access controls
- Performing security vulnerability scans
- Analyzing physical access to the systems

Monitoring

It describes the process of threat and data breach detection.

Defining the behavior types to trigger alerts

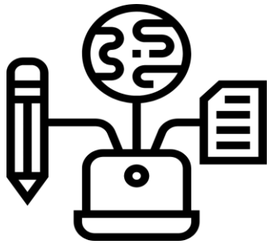


Taking actions on alerts as needed

Patch Management

It involves acquiring, testing, and installing multiple patches to an administered computer system.

Patch Management Tasks



Maintain knowledge of available patches

Decide appropriate patches for particular systems

Ensure that patches are installed properly

Test systems after installation

Document all associated procedures

Patch Management: Example

The outbreak of WannaCry ransomware became large and intense because of a missing security patch.

System Hardening

It is a collection of tools, techniques, and best practices to reduce vulnerability.

Technology applications

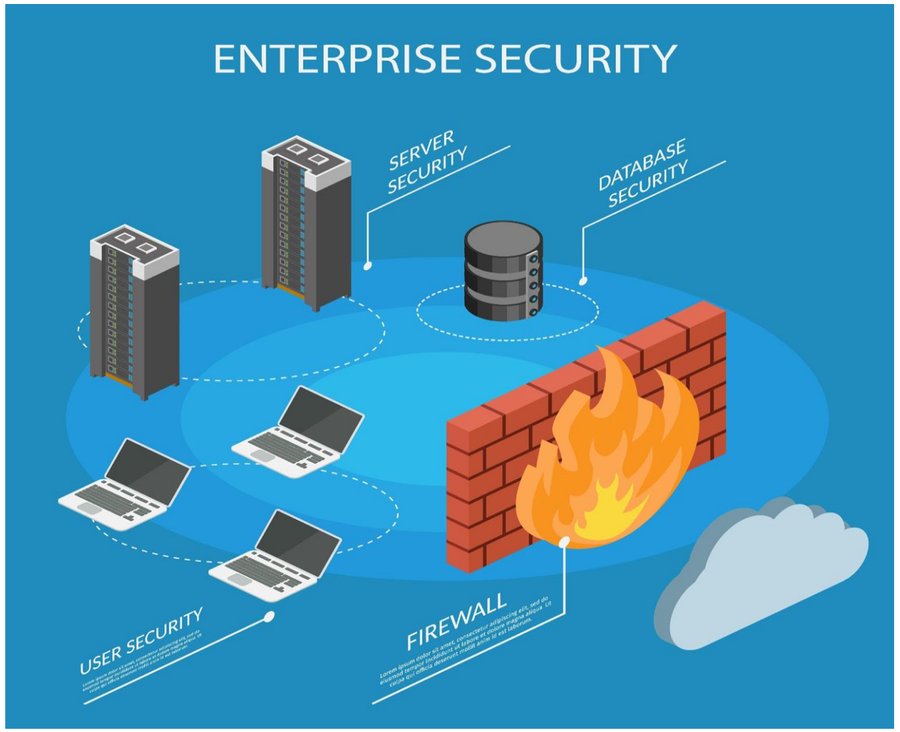
Systems

Infrastructure

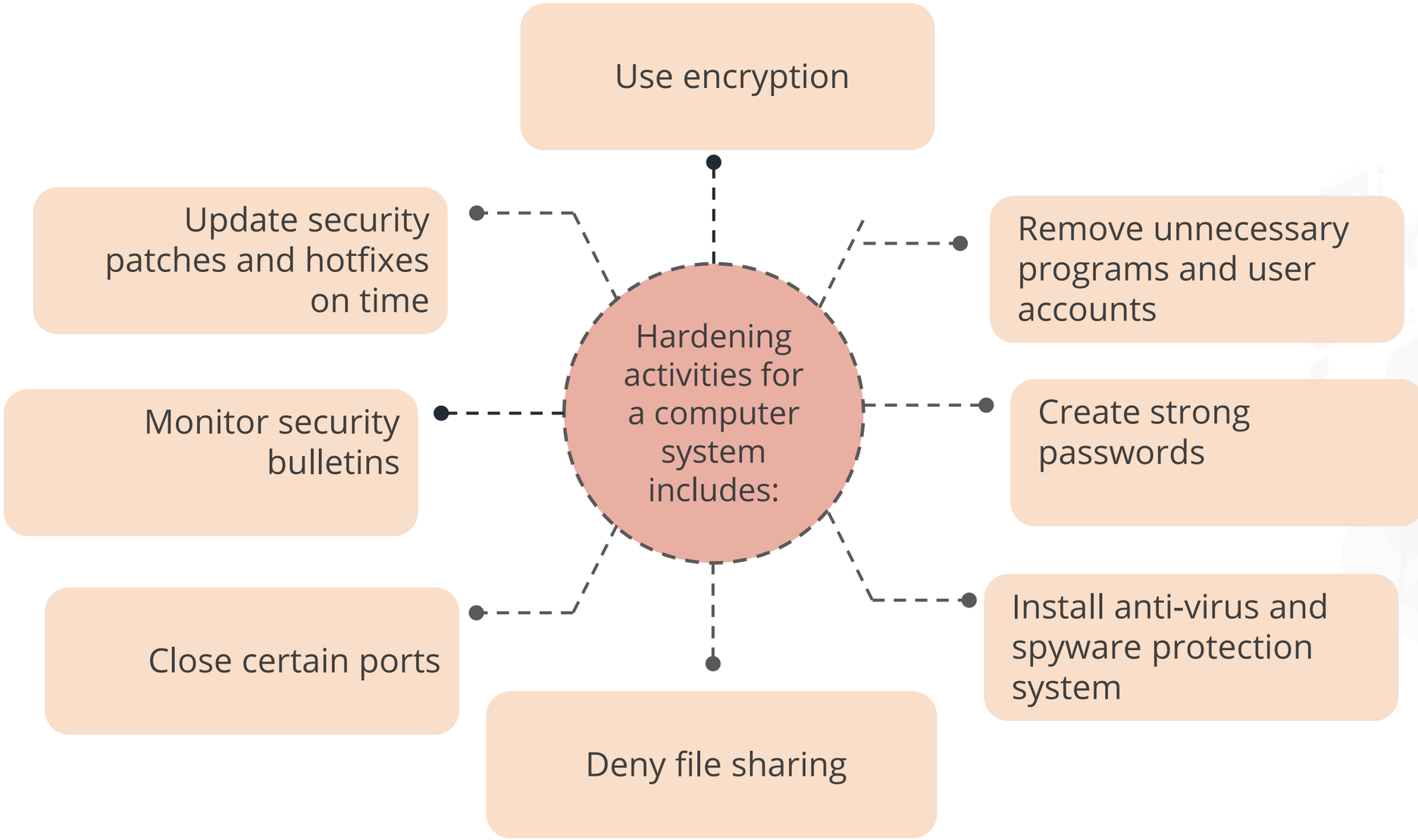
Firmware

System Hardening: Purpose

It eliminates security risks and secures a system by reducing its attack surface.



System Hardening Activities



Change Control

It is a systematic approach to manage all changes made to a product or system.

Change Control: Purpose

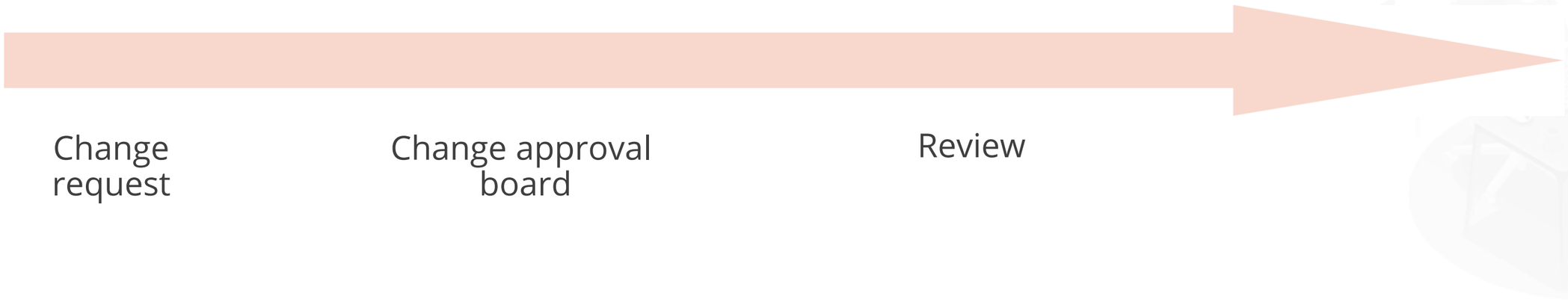
All changes are documented

No unnecessary changes are made

Services are not disrupted

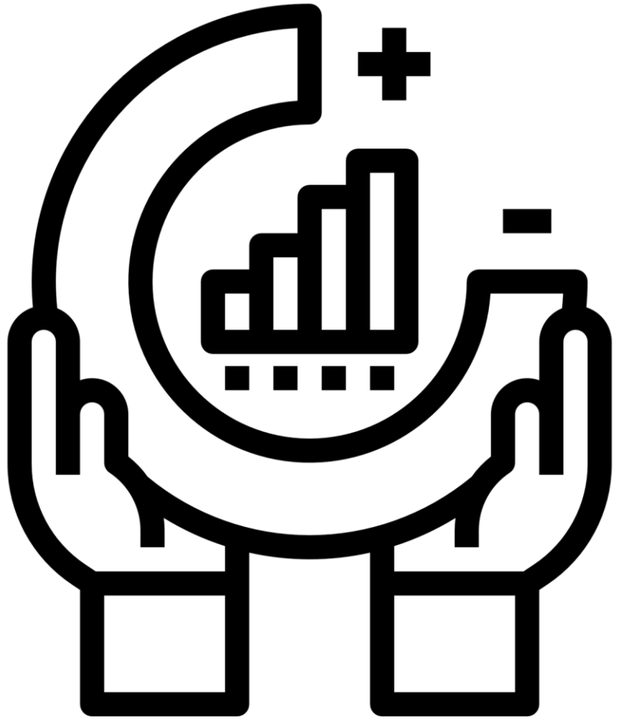
Resources are used efficiently

Change Control: Purpose

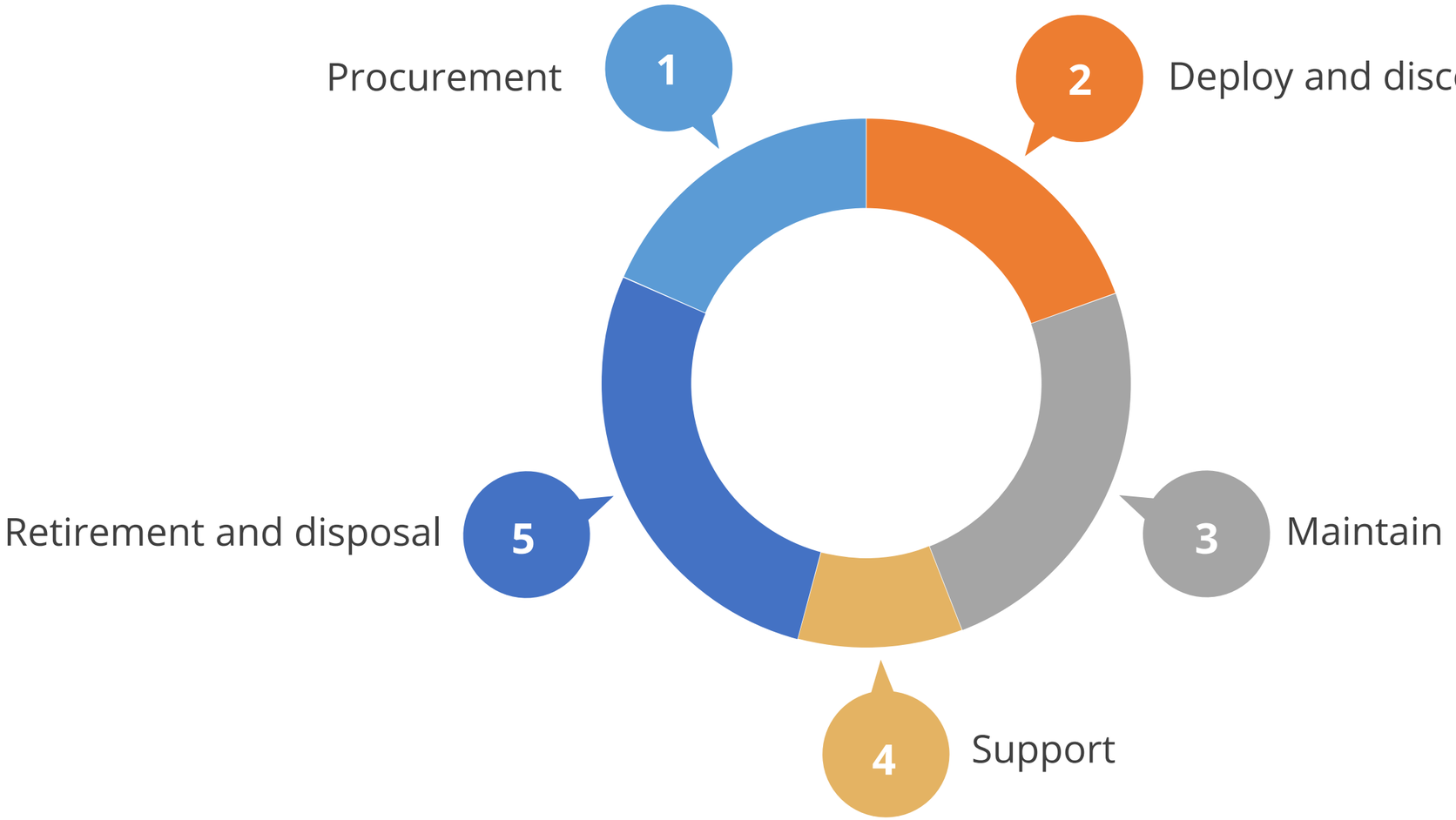


Asset Management

It is the systematic process of developing, operating, maintaining, upgrading, and disposing of assets cost-effectively.



Asset Management Lifecycle



Data Management

Data is the smallest piece of information in any form.

Text documents

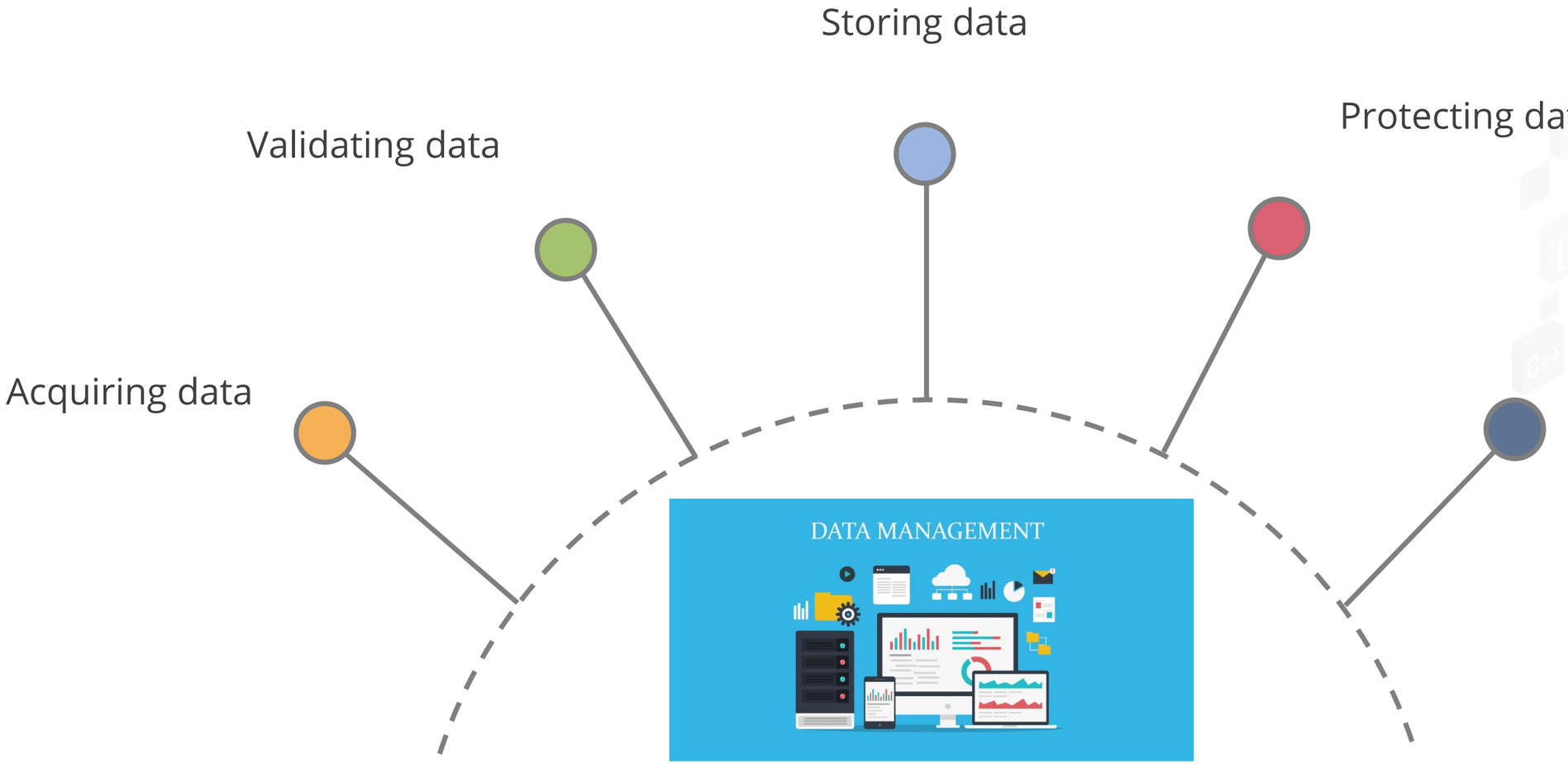
Images

Audio clips

Software programs

Data Management

It is an administrative process to ensure the accessibility, reliability, and timeliness of the data for its users.



States of Data

They describe the different modes whereby data is used by a computing equipment.

Three Basic States of Data

Data at rest

Data in transit

Data in use

Information Lifecycle

Acquisition: Indexed system data

Disposal: Stored data for destruction

Archival: Backup, protection, and retention

Use: Challenges in protection

Information Lifecycle

It is an ongoing process

It helps ensure data is protected

Metadata must be at the right classification level

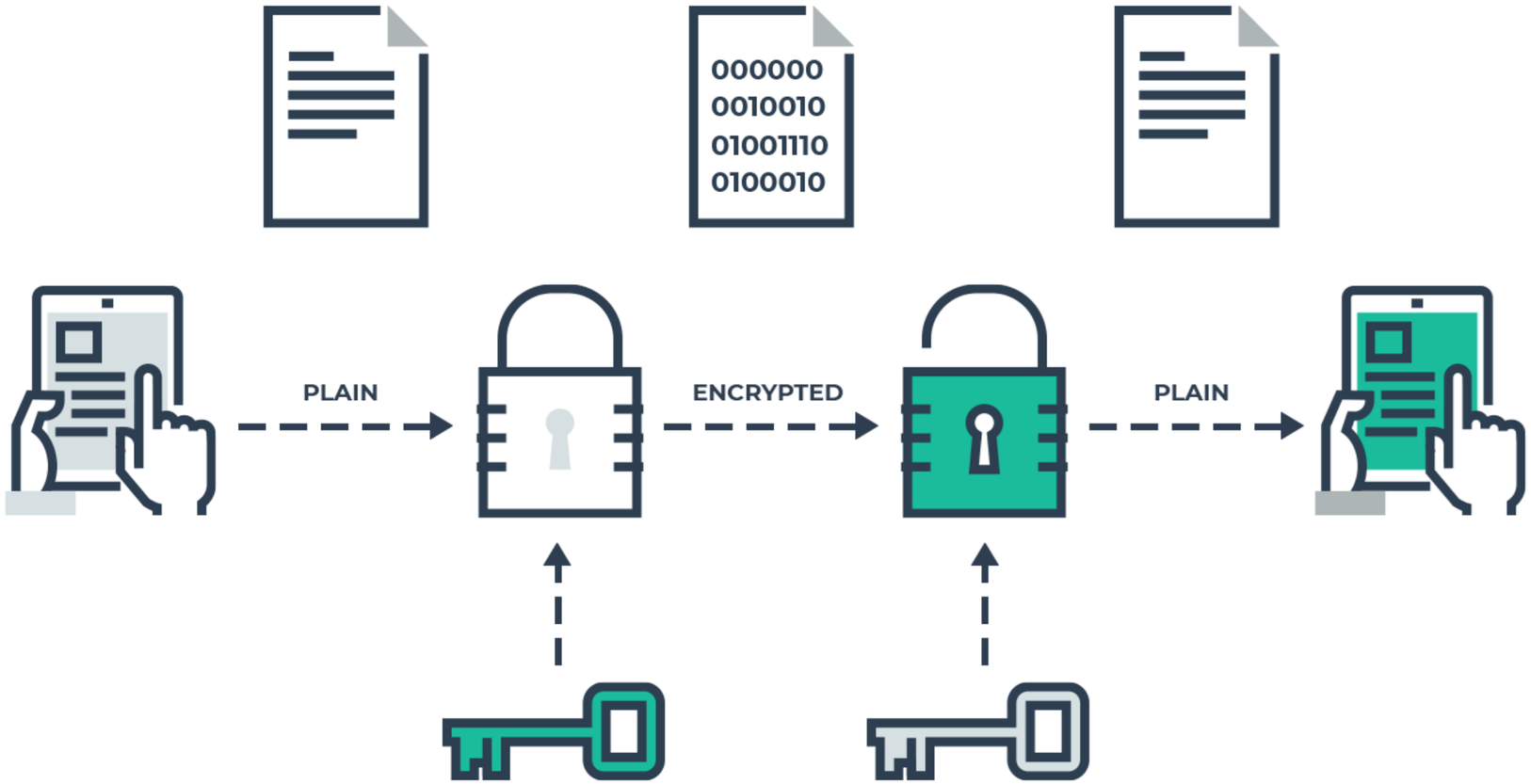
It helps indicate the level of data protection

Classification level must be attached to the information lifecycle

Encryption

It describes the different modes whereby data is used by a computing equipment.

Encryption



Encryption

Protects data in transit over networks

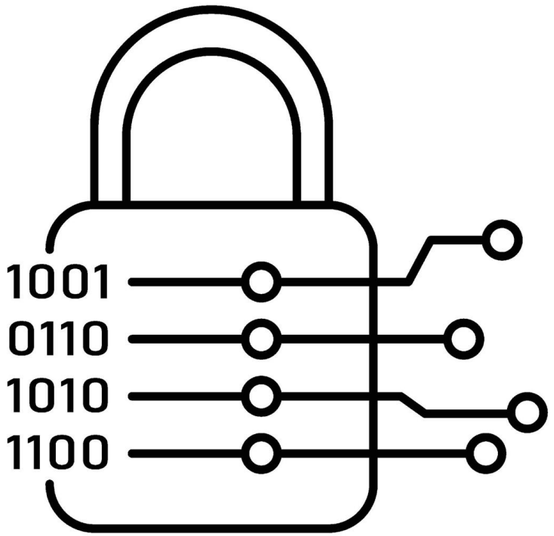
Protects information stored on computers

Deters and detects alterations of data

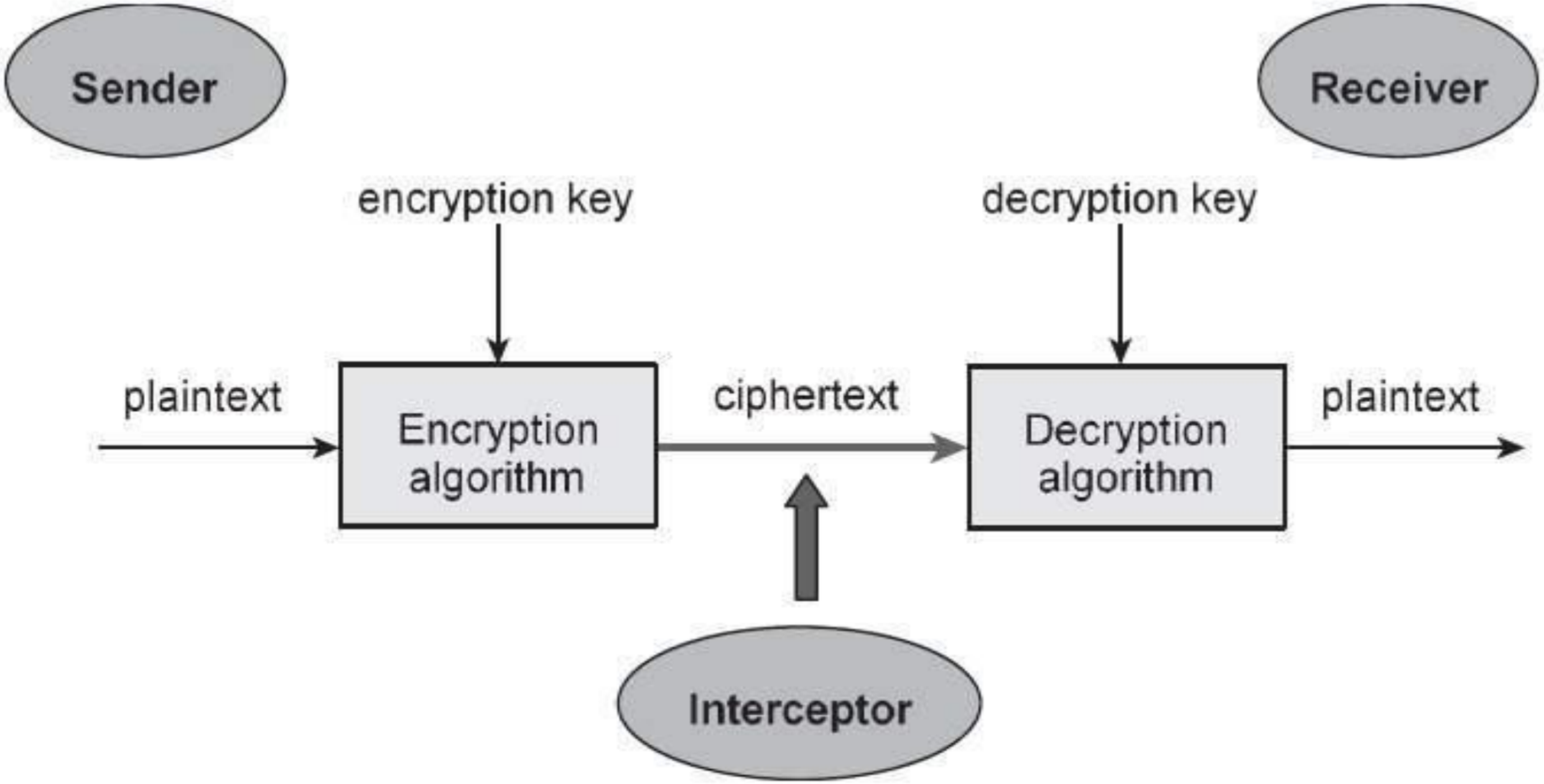
Verifies the authenticity of a transaction

Cryptography

Cryptography is the science of protecting information by encoding it into an unreadable format.



Cryptography



Factors Influencing Effective Encryption

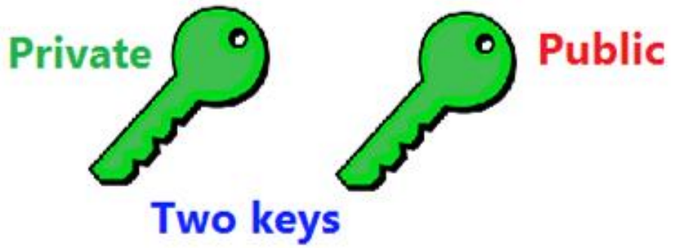
The non-existence of back doors

Algorithm strength, secrecy, and difficulty of compromising a key

The inability to decrypt an entire cipher text

Types of Encryption

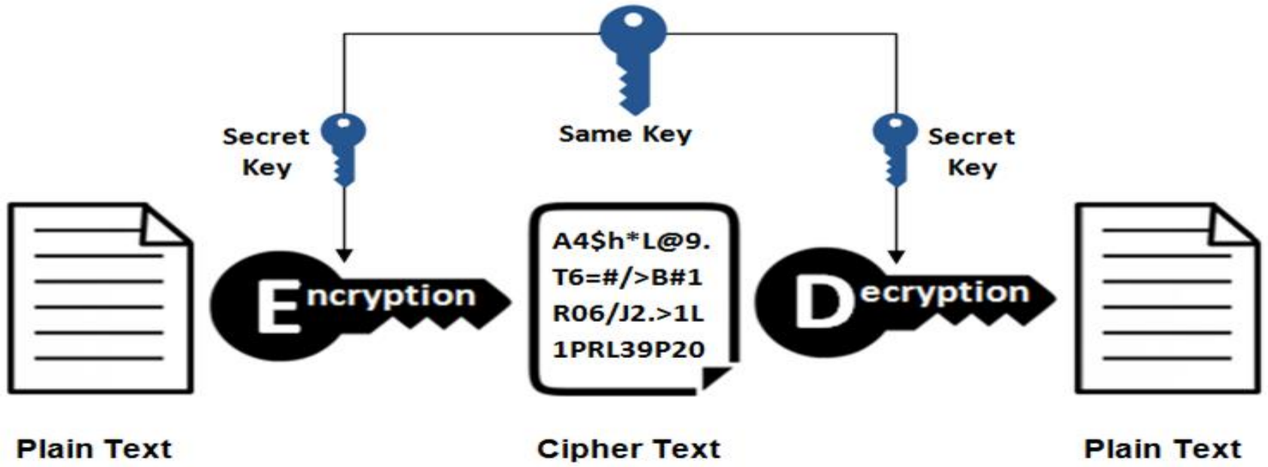
Symmetric Encryption



Asymmetric Encryption

Symmetric Encryption

Symmetric encryption is based on the same key or private key to encrypt plain text and decrypt ciphertext.



- Uses one key to encrypt and decrypt
- Uses less processing power

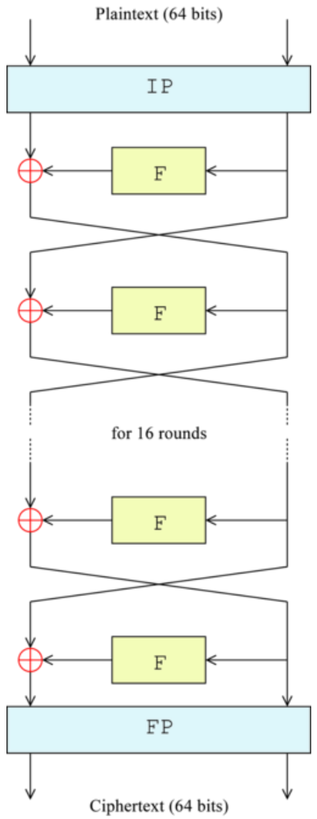
- Shares the key with the receiver

Symmetric Encryption

Common private key cryptography systems:

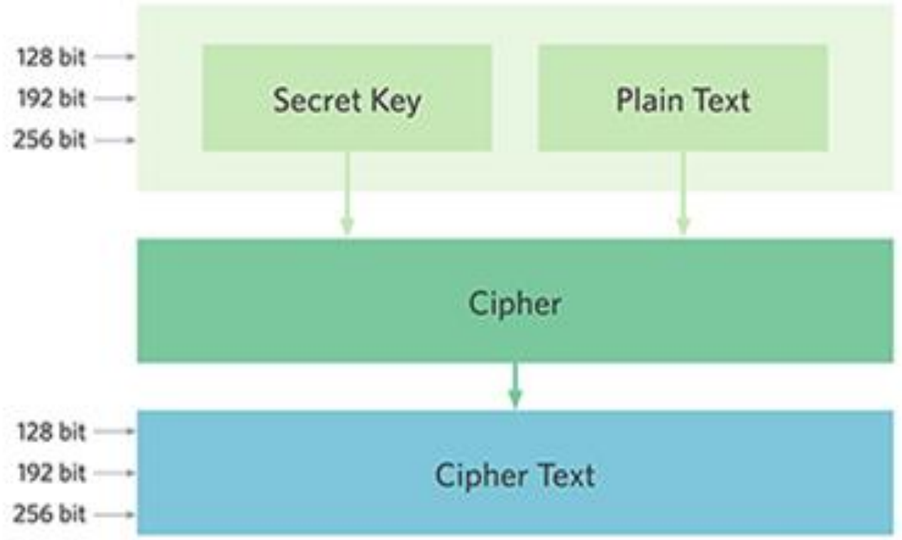
Data Encryption Standard (DES)

64-bit

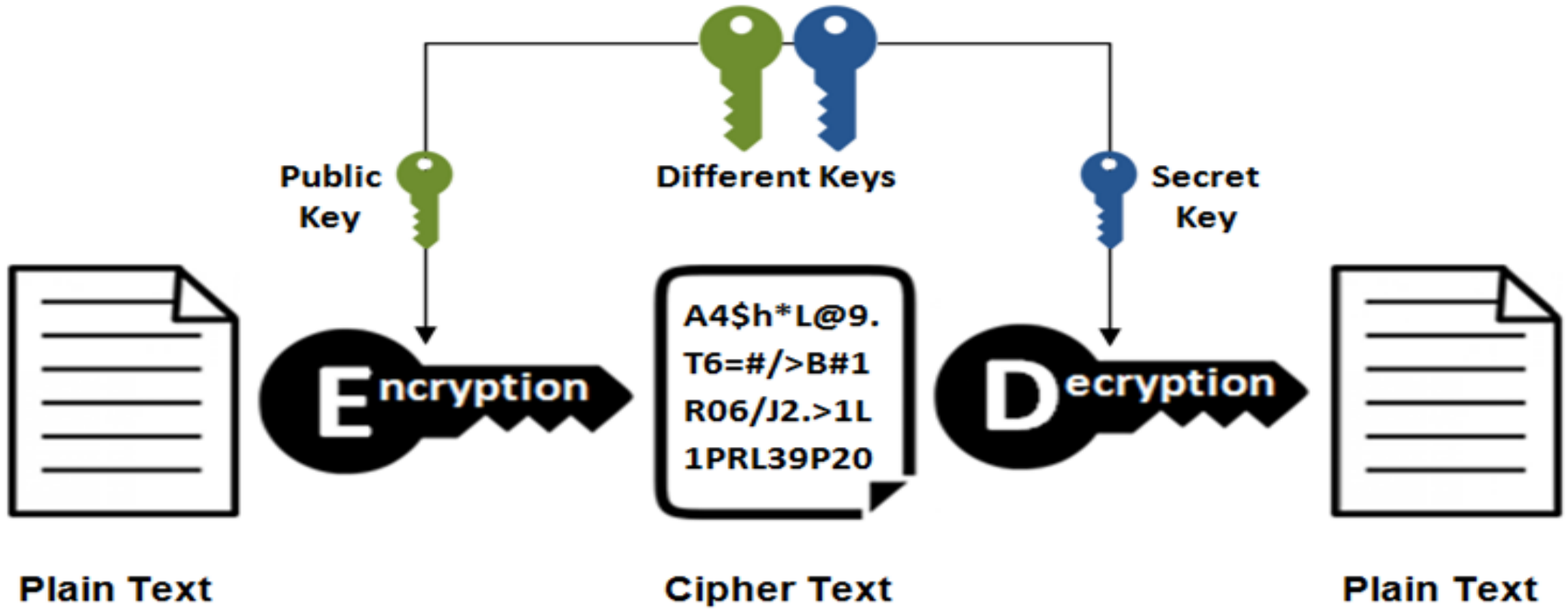


Advanced Encryption Standard (AES)

128-bit to 256-bit



Asymmetric Encryption



Solves the problem of sharing the key with the receiver

Asymmetric Encryption

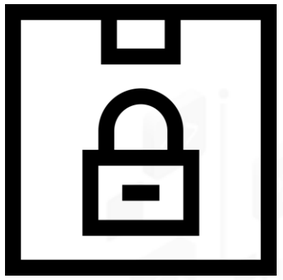
Services of cryptography:

Authentication

Validates the sender's identity

Non-repudiation

Prevents denial of action



Confidentiality

Controls who reads the data

Incident Response

It is an organized approach to address and manage the aftermath of a security breach.

Incident Response: Goals

Reduces damage, recovery time, and costs

Manages potential disruption to IT service

Has normal service operations within SLAs

Minimizes the adverse impact on business operations

Security Training

It is an organized approach to addressing and managing the aftermath of a security breach or cyber attack.

Security Awareness

It is the process of exposing people to security issues so that they may be able to recognize them and better respond to them.

Key Takeaways

- Cybersecurity refers to a set of techniques used to protect the integrity of network programs and data from attack, damage, and unauthorized access.
- Malware is a software that is designed to cause damage to a computer, server, client, or network. The types of malware include worm, spyware, virus, trojan, and logic bomb.
- Strategic plan, tactical plan, and operational plan are the types of security management plans.
- Change control is a systematic approach for managing all changes made to a product or system.